International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.35-44
http://dx.doi.org/10.14257/ijsia.2017.11.1.04

Research on Data Security Mechanism among Cloud Services based on Software Define Network

Zhao Wenbin[1], Fan Tongrang[2*] and Wang Hongsheng[3]

[1,2,3] *School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, Hebei 050043, China*
[1]*zhaowb.email@qq.com*, [2*]*fantr@stdu.edu.cn*,

Abstract

In cloud services, users' data and applications are stored in remote cloud servers, their safety and security can be guaranteed by their cloud servers, but it is difficult for guarantee their security in interaction among them. As software defined network arise, its architecture realizes the separation between control plane and data plane, provide a promising way of dealing with privacy leakage of cloud data. This paper study a data security mechanism among cloud service based on software define network architecture, which maintains security policy on SDN controller cluster, which controls forwarding based on the mapping between physical network and logic network. This mechanism contains data service provider, data service user and privacy service provider. Data service provider customizes data attribute restriction based on data security protection requirements. Privacy service provider which is realized based on SDN controller, is responsible for the security of data interacting between data service user and data service provider, such as identity authentication, source data partition and data block recovering in accordance with data attribute restriction. Data service provider stores source data on cloud server. Through experiments and analysis, this data security mechanism is effective and feasible.

Keywords: *Data Security, Cloud Service, Software Define Network, Data Partition, Identity Authentication*

1. Introduction

In cloud platforms, many applications and data are both deployed at cloud server, so cloud data security has become an important factor that hinders the development of cloud platforms [1]. For cloud services, their security not only depends on dynamic deployment, configuration and management of security policy and security components, but also depends on the awareness, decision and response of network security system. Software define network realizes the separation between control plane and data plane, and controls network equipments related with cloud data center based on network topology, network status and security incident, so can provide a logical resource pool of distributed security ability, which is a service of security[2]. This paper study a data security mechanism among cloud service based on software define network architecture, which maintains security policy on SDN controller cluster, which controls forwarding based on the mapping between physical network and logic network. This mechanism contains data service provider, data service user and privacy service provider. Data service provider customizes data attribute restriction based on data security protection requirements. Privacy service provider which is realized based on SDN controller, is responsible for the security of data interacting between data service user and data service provider, such as

*Fan Tongrang is the corresponding author.

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2017 SERSC

identity authentication, source data partition and data block recovering in accordance with data attribute restriction. Data service provider stores source data on cloud server.

2. Related Work

2.1. Cloud Data Privacy Protection

In cloud service, data is saved and processed on cloud servers, so cloud service providers, which have high trust, can be responsible for its security. But the data transmission among different cloud service providers insecurity is not security, so many researches are carried out [3].

With encryption, local data is uploaded to remote cloud server. This data protection method needs to solve some key technology，such as data retrieval, data encryption, and data decryption[4].According to the characteristics of cloud computing, some scholars have proposed keyword retrieval method based on symmetric encryption cipher text, supports data service provider part decryption work reduce DReq computing and network traffic, supports encrypted search[5]. For enterprise cloud computing users in data management and data-sharing issues, proposed after the encrypted data in the cloud to build encryption key index tree to support encrypted data to retrieve, control user authentication for data sharing[6]. For data management in the cloud, and all right, scholars have been designed based on partition of data protection mechanisms, data is divided into small blocks, small data block to be saved to a local, large blocks of data to the cloud storage system, cloud data encrypted according to the user's security level[7]. For Bloom Filer optimization of redaction retrieved method, due to its only support precise string match, in actual situation Xia format inconsistent will inevitable, so feasibility is unlikely to, for subsequently proposed of support encryption string fuzzy retrieved programme, using edit distance to quantitative string of similar degrees, and for each string additional a based on pass distribution breaks of fuzzy string group, using multiple precise match to achieved fuzzy retrieved, This programme supports only the "all or nothing" query, query structure cannot be sorted[8]. Then scholars was designed based on vector and matrix operations of encryption schemes can be calculated, using the vector and matrix operations, data encryption, and support for encrypted string of fuzzy retrieval and encrypted numeric data mathematical operations[9].

Database by data privacy protection, scholars have suggested that data block optimization algorithm using longitudinal Division of the methods on the relational database partitioning, first user privacy will be compromised by a single property to a local storage of data, and privacy constraints 2- Coloring method into two categories of data property, and set the property to a class to the server, set the property to a little, along with individual privacy properties are stored to a local[10]. Another scenario is a data table is divided into two pieces, one of them stored to the client, another part of the store to the server[11]. Block matrix then proposed, according to the number of attributes of the user property sheet, property size, frequency of queries, queries, and so on make-weight matrix[12]. According to the weights get table partitioning method[13].

Scholars based on the relationships between the data slice confusion method and data counterfeiting methods, block after block of data confused first, then check the block meets the distribution proposed property values, and then make the data falsification, and data integrity verification mechanisms [14]. Multiuser shared database then realizes a more user data partition divides the data model[15]. But the block number of the data partition for data reconstruction has a certain influence, smaller number of blocks of data is very important to improve the efficiency of data processing, research does not verify the number of data blocks to a minimum [16].

 Copyright ⓒ 2017 SERSC

2.2. Software Defined Network Architecture

SDN architecture has the following advantages: high scalability/high flexibility of network deployment, fine and efficient data flow control, *etc*[17]. SDN provide to centralized network equipment, automated management, and unified strategy execution, compared to the current network architecture to improve the reliability and security[18]. Traditional network security applications, such as access control, firewall, invasion detection and defense intruding can also use SDN controller of open API implementation or easily integrated into SDN[19].

As mentioned above, SDN architecture provides a platform, can provide security for it, and provide security services. Most researchers believe that the current network security technology of accumulation completely can be competent the security requirements of SDN, as Gloria proposed SDN security technology architecture and the traditional network security technology architecture basically no difference[20]. What kind of security mechanism, but the specific provide how to design, implementation. Hartman think SDN security requirements such as Wasserman M mainly occurred in the application layer and control layer, including application of authorization, authentication, isolation, and strategy of conflict resolution[21]. Hartman and Wasserman M et al. discusses the three kinds of authorization, authentication mechanism used in the possibility of SDN, especially in the case of cross-domain[22].first, through a proxy authentication; Second, direct distribution of cross-domain authentication credentials (such as symmetric key, private key certificate, *etc*.);Third, through joint certification (such as OAuth01 ABFAB1).One final way that united authentication, has the characteristics of flexible, easy to use in a variety of occasions[23]. But this does not give reference request, ABFAB in concrete application way of SDN. Shin S put forward a development network security application on SDN architecture development environment FRESCO, FRESCO "itself as an application of SDN application layer, the security of the operation in the above mentioned reinforcing the control layer of operating system (enhanced NOX).

3. Data Security Model among Cloud Services based on Software Define Network

Data security model among cloud services based on software define network include: data service user DSU, data service provider DSP and privacy service provider PSP. Their function and relationship is shown in Figure 1.

The transmission of cloud data, which includes data uploading and data accessing, mainly exists between data service user and data service provider.

The processing of data uploading is as follows:

(1) New Data service provider registers with privacy service provider, and gets respectively authorization of data storing service and privacy protection service.

(2) According to demand of data storing and privacy protection, data service user produce data property description sheet and privacy protection rule, and sent to privacy service provider.

(3) Privacy service provider produces data partition policy and privacy protection policy to meet data service user’s demand.

(4) Based on data partition policy and privacy protection policy, privacy service provider partition source data, which is uploaded by data service user, and sends partition data to data service provider.

Copyright ⓒ 2017 SERSC

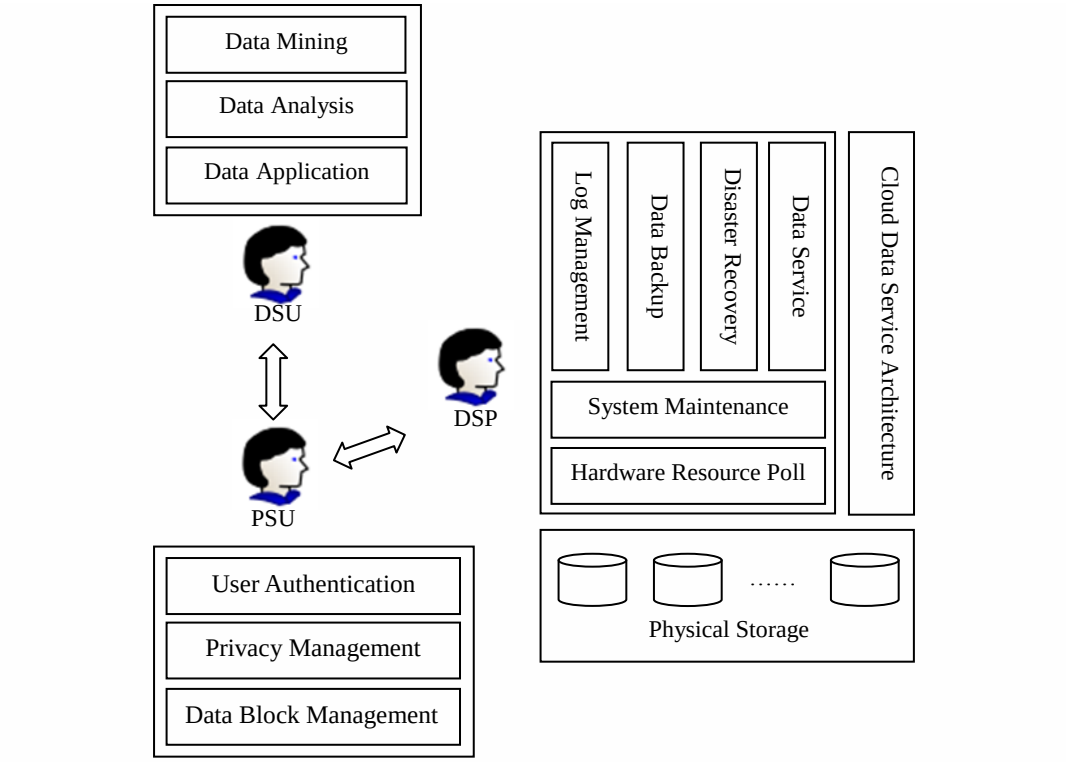


Figure 1. The Function and Relationship in Data Security Model

The processing of data accessing is as follows:

(1) Data service user get identity authentication from privacy service provider.
(2) Privacy service provider determines whether the access request sent by data service user is satisfied privacy protection policy. If satisfy, send this request to data service provider, if not, discard this request.
(3) Based on access request, data service provider send partition data result to privacy service provider.
(4) By data partition policy, privacy service provider recovery partition data to source data.

3.1. Identity Authentication

When data service provider registers with privacy service provider, they generate a pair of keys and send public key to each other. Then data service user authenticates identity for privacy service provider with public key. The process of identity authentication between data service user and privacy service provider is shown as Figure 2.

(1) Data service user send authentication request to privacy service provider.

(2) Privacy service provider generates a random number 1 based on user's information, encrypts number 1 with own private key and sends to data service user.

(3) Data service user decrypts received encrypted random number 1 with provider's public key. Data service user generates a random number 2, encrypts number 1 and number 2 with own private key and sends to privacy service provider.

(4) Privacy service provider decrypts received encrypted random number 1 and number 2 with user's public key. If source number 1 is same as decrypted number 1, privacy service provider encrypts number 2 with own private key and sends to data service user, or authentication is denied.

 Copyright ⓒ 2017 SERSC

(5) Data service user decrypts received encrypted random number 2 with provider's public key. If source number 2 is same as decrypted number 2, authentication is accepted, or denied.

(6) Data service user get permission to sends service request to privacy service provider.

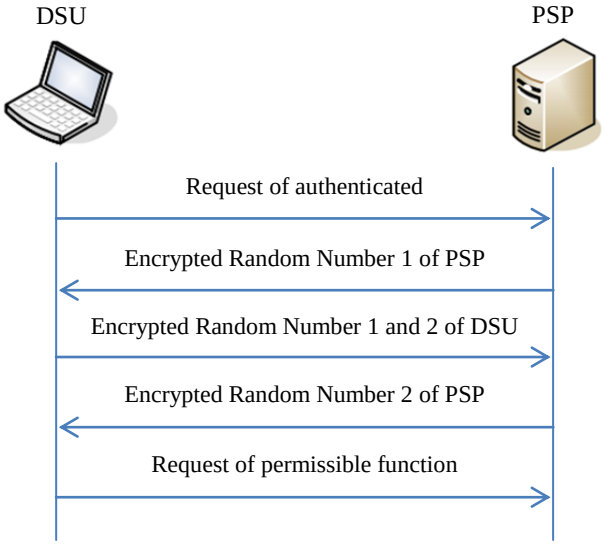


Figure 2. The Process of Identity Authentication between DSU and PSP

3.2. Network Framework of Data Security Model

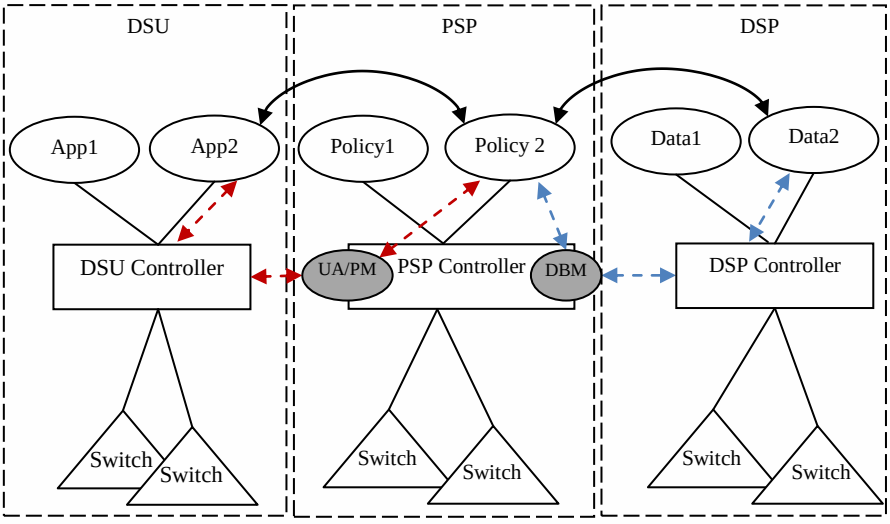


Figure 3. The Network Framework of Data Security Model

In network framework of data security model, the interaction among data service provider, data privacy provider and data service user depend on the software defines network controllers, show as Figure 3. The core controller is the data privacy provider's controller, which include data block management, privacy management and user authentication.

The function of data block management contains:

Copyright ⓒ 2017 SERSC

(1) Data partition policy is produced based on data property description sheet made by data service user.

(2) Source data is partitioned to data block, and data block is send to data service provider.

(3) Data block is recovery to source data, and source data is send to data service user.

The function of privacy management is that privacy protection policy is produced based on privacy protection rule made by data service user.

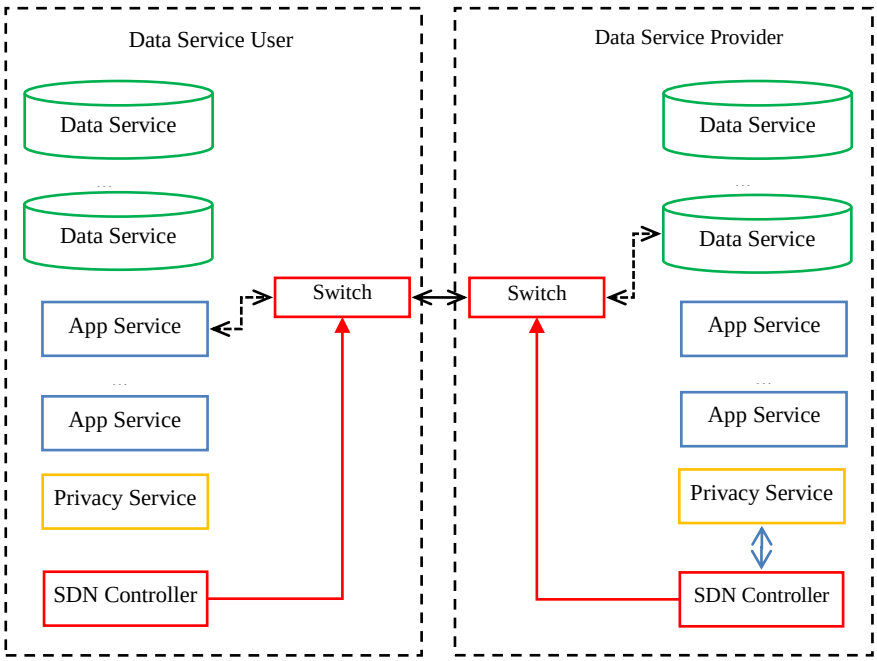


Figure 4. The Realization of Data Security Model's Network Framework

The realization of data security model's network framework is shown in Figure 4. Data service user and data service provider are deployed on different cloud platform, privacy service provider is deployed the cloud platform of data service provider. SDN controller manages network of cloud platform, such as connection, flow, route and so on. Especially, SDN controller network can adjust network connection based on privacy service.

4. Data Partition

In this paper, cloud data is analyzed from three aspects: Attribute Combination Privacy Restriction Set ACPRS, Attribute of Individual Protection Set AIPS, and None Attribute Privacy Restriction Set nAPRS[29]. So the main idea of data partition is that according to ACPRS provided by DSP, data is divided into two blocks: AIPS and nAPRS with ACPRS adjacency matrix and graph coloring theory.

Attribute combination of privacy restriction contains {Name, Addr}, {Name, Ill}, {Name, DoctorSSN}, {Addr, Ill}, {Addr, DoctorSSN}, and Attribute of Individual Protection contains {Tele}. So DSU can provide ACPRS, AIPS and nAPRS, ACPRS={Name, Addr, Ill, DoctorSSN}, AIPS={Tele}, NAPRS={SSN, Sex, Age}. According to attribute combination of privacy restriction, ACPRS adjacency matrix is built, as shown in Table 1.

Copyright ⓒ 2017 SERSC

Table 1. ACPRS Adjacency Matrix

Attribute	Name	Addr	Ill	DoctorSSN
Name	0	1	1	1
Addr	1	0	1	1
Ill	1	1	0	0
DoctorSSN	1	1	0	0

An undirected graph, which takes Attribute of ACPRS as node and attribute combination of privacy restriction as edge is constructed based on ACPRS adjacency matrix. An undirected graph is processed by graph coloring theory, as shown in Figure 5.

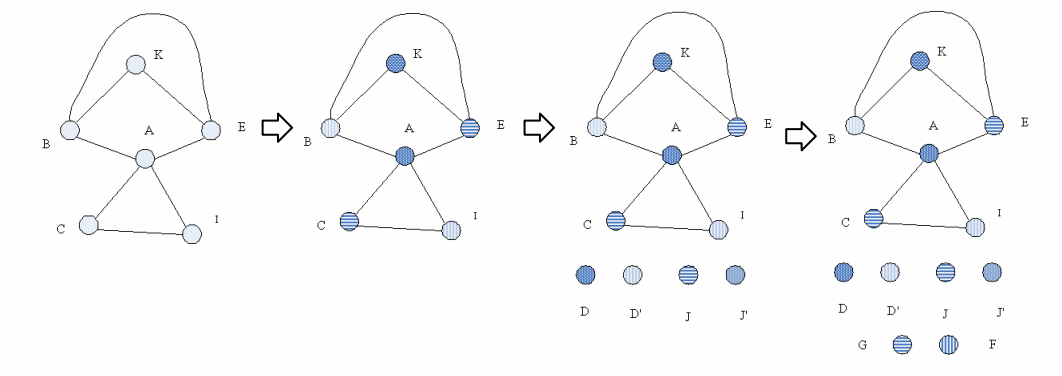


Figure 5. The Process of Data Partition

Table 2. Cloud Servers Configuration

Host Name	Functionality	IP Address	DNS Servers	Gateway IP
server1(DSP)	All components of OpenStack including nova-compute	eth0: Public N/W 10.0.0.101 eth1: Private N/W 192.168.65.1	202.206.32.1 202.206.32.2	10.0.0. 1
server2(DSP)	Nova-compute	eth0: Public N/W 10.0.0.102 eth1: Private N/W 192.168.65.2	202.206.32.1 202.206.32.2	10.0.0. 1
server1(DSU)	All components of OpenStack including nova-compute	eth0: Public N/W 10.0.1.101 eth1: Private N/W 192.168.65.1	202.206.32.1 202.206.32.2	10.0.1. 1
server2(DSU)	Nova-compute	eth0: Public N/W 10.0.1.102 eth1: Private N/W 192.168.65.2	202.206.32.1 202.206.32.2	10.0.1. 1

5. Experiment

For proposed data security mechanism, this paper carries on experiments, which adopts OpenStack to build cloud platform, and use Hadoop to realize cloud service.

The cloud platform of data service provider and data service user use HuaWei servers, which own CPU: Xeon E5-2620V2 2.1GHz, Memory: DDR3 32G, Disk: 320G. The configuration of cloud platform is shown as Table 2.

Copyright ⓒ 2017 SERSC

On the cloud platform of data service provider, DataNode of Hadoop is deployed, which is responsible for reading and writing of HDFS data. NameNode, JobTracker and TaskTracker are deployed on the cloud platform of data service user.

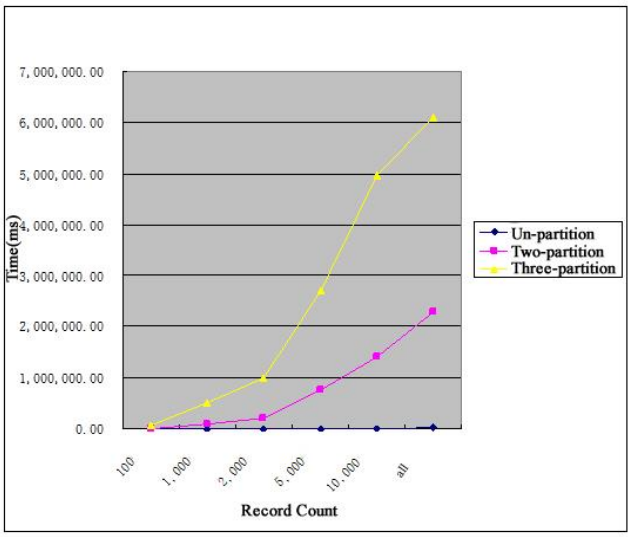


Figure 6. The Comparison of Data Partition's Query Time

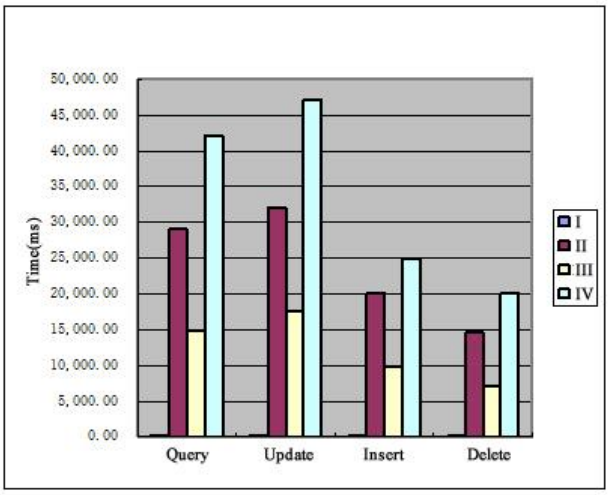


Figure 7. The Comparison of Database Operation Time

For data query, the experiment compared for un-partition data and partition data, as shown in figure 6. When query is executed 100 instances and the number of query data is 100, 1000, 2000, 5000, 10000 and all, the total time is recorded. The result shows that the query of un-partition data is more efficient than other. For partition data, the largest execution time is 61 087.42 ms, this can meet the needs of large data query.

Efficiency is an important indicator for testing the proposed mechanism. Experiment data, which contain 1,000,000 records in data table, is performed with different database operations and different storage methods. The result is compared as shown in Figure 7.

In Figure 7, I, II, III and IV represent original table, split table, split encrypted table and the proposed mechanism. Database operations contain query, update, insert and delete. The time of original table's operation is much less than other, because these operations take some time to other process such as split, encrypt, *etc*. for other three methods. The time of the propose mechanism is more than split table, but less than split

 Copyright ⓒ 2017 SERSC

encrypted table, meanwhile the propose method provide security preserving for cloud data privacy.

5. Conclusion

For data security among cloud service, this paper proposes a data security mechanism based on software defined network. In proposed mechanism, security policy is maintains on SDN controller, which controls forwarding based on the mapping between physical network and logic network. Based on data property description sheet and privacy protection rule customized by data service provider, privacy service provider partition source data and sends split data to data service provider. Experiment shows the proposed mechanism can effectively prevent the leakage of privacy information. In future, the study of data reconstruction strategy, data processing time will be carried on to improve the efficiency of cloud data security mechanism.

Acknowledgement

This study is funded by the National Natural Science Foundation of China (#61373160).

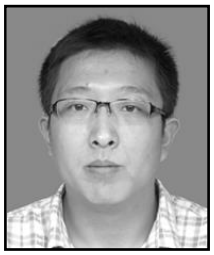
References

[1] Hacigumus H, Iyer B, Mehrotra S. Providing database as a service[C]. Data Engineering, 2002. Proceedings. 18th International Conference on. IEEE, 2002: 29-38.
[2] Sgambelluri A, Giorgetti A, Cugini F, Paolucci F, Castoldi P. Openflow-Based segment protection in ethernet networks. IEEE/OSA Journal of Optical Communications and Networking, 2013,5(9):1066−1075.
[3] Aggarwal G, Bawa M, Ganesan P, et al. Two can keep a secret: A distributed architecture for secure database services[J]. CIDR 2005, 2005.
[4] Ciriani V, Di Vimercati S D C, Foresti S, et al. Keep a few: Outsourcing data while maintaining confidentiality[M]. Computer Security–ESORICS 2009. Springer Berlin Heidelberg, 2009: 440-455.
[5] Samarati P, di Vimercati S D C. Data protection in outsourcing scenarios: Issues and directions[C]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 1-14.
[6] Zhang K, Shi Y, Li Q, et al. Data privacy preserving mechanism based on tenant customization for saas[C]. Multimedia Information Networking and Security, 2009. MINES'09. International Conference on. IEEE, 2009, 1: 599-603.
[7] Shi Y, Zhang K, Li Q. A new data integrity verification mechanism for SaaS[M] . Web Information Systems and Mining. Springer Berlin Heidelberg, 2010: 236-243.
[8] Zhang K, Li Q, Shi Y. Data privacy preservation during schema evolution for multi-tenancy applications in cloud computing[J]. Web Information Systems and Mining. Springer Berlin Heidelberg, 2011: 376-383.
[9] Shen Y, Cui W, Li Q, et al. Hybrid Fragmentation to Preserve Data Privacy for SaaS[C]. 2011 Eighth Web Information Systems and Applications Conference. IEEE, 2011: 3-6.
[10] Li L, Li Q, Shi Y, et al. A new privacy-preserving scheme DOSPA for SaaS[M] . Web Information Systems and Mining. Springer Berlin Heidelberg, 2011: 328-335.
[11] Zhao, Wenbin, Zhao, Zhengxu. Research on engineering software data formats conversion network[J]. Journal of Software. 2012, 7(11): 2606-2613
[12] Krishna R K N, Sayi T, Mukkamala R, et al. Data outsourcing in cloud environments: a privacy preserving approach[C]. Proceedings of the 2012 Ninth International Conference on Information Technology-New Generations. IEEE Computer Society, 2012: 361-366.
[13] Qin Liu,GuojunWang,JieWu. Secure and privacy preserving keyword searching for cloud storage services[J]. Journal of network and computer applications, 2012, 35(3):927-933
[14] Shu Qin Ren,Khin Mi Mi Aung. PPDS:Privacy Preserved Data Sharing Scheme for Cloud Storage[J]. International Journal of Advancements in Computing Technology , 2012,4(16): 493-499.
[15] Qin Liu,GuojunWang,JieWu. Secure and privacy preserving keyword searching for cloud storage services[J]. Journal of network and computer applications, 2012, 35(3):927-933
[16] Shu Qin Ren,Khin Mi Mi Aung. PPDS:Privacy Preserved Data Sharing Scheme for Cloud Storage[J]. International Journal of Advancements in Computing Technology , 2012,4(16): 493-499.

Copyright ⓒ 2017 SERSC

[17] Syrivelis D, Iosifidis G, Delimbasis D, Chounos K, Korakis T, Tassiulas L. Bits and coins: Supporting collaborative consumption of mobile Internet. In: Proc. of the IEEE INFOCOM. Washington: IEEE Computer Society Press, 2015.
[18] Ongaro F, Cerqueira E, Foschini L, Corradi A, Gerla M. Enhancing the quality level support for real-time multimedia applicationsin software-defined networks. In: Proc. of the 2015 Int'l Conf. on Computing, Networking and Communications (ICNC).Washington: IEEE Computer Society Press, 2015. 505−509.
[19] Li J, Chang X, Ren Y, Zhang Z, Wang G. An effective path load balancing mechanism based on SDN. In: Proc. of the 13th Int'lConf. on Trust, Security and Privacy in Computing and Communications (TrustCom). Washington: IEEE Computer Society Press,2014. 527−533.
[20] Thorat P, Raza SM, Nguyen DT, Im G, Choo H, Kim DS. Optimized self-healing framework for software defined networks. In:Proc. of the 9th Int'l Conf. on Ubiquitous Information Management and Communication. New York: ACM Press, 2015. 1−6.
[21] Luo M, Zeng Y, Li J. An adaptive multi-path computation framework for centrally controlled networks. In: Proc. of the Computer Networks. Elsevier, 2015. 30–44.
[22] Van Adrichem NLM, Van Asten BJ, Kuipers F. Fast recovery in software-defined networks. In: Proc. of the 3rd EuropeanWorkshop on Software Defined Networks (EWSDN). Washington: IEEE Computer Society Press, 2014. 61−66.
[23] Capone A, Cascone C, Nguyen AQT, Sansò B. Detour planning for fast and reliable failure recovery in SDN with OpenState. arXiv:1411.7711, 2014.

Authors



Zhao Wen-bin, born in 1985, Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. His major field of study is network technology and information processing. Email address: zhaowb.email@qq.com.

Fan Tong-rang, born in 1965, Professor. Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. Her main research interest include network technology and Information processing. Email address: fantr@stdu.edu.cn; fantr2009@126.com.

 Copyright ⓒ 2017 SERSC