ISSN:2348-2079

JAN-2016

International Journal of Intellectual Advancements and Research in Engineering Computations

AN EFFICIENT PRIVACY PROTECTION METHOD FOR RAIN CLOUD COMPUTING

*[1]S.Rajpriya, [2]S.Jagadeesan

ABSTRACT

Cloud computing is an evolving term for anything that involves delivering hosted services over the Internet. In cloud environment, data security and privacy is consistently a major issue due to outsourcing organizational sensitive information into cloud. In order to carry out privacy protection causes enormous operating cost. Thus it is a serious issue to achieve the most suitable protection to turn down performance utilization while present privacy protection. In this paper, the Efficient Privacy Protection method (EPPM) is proposed to afford the suitable privacy protection which is fulfilling the user demand privacy constraint and maintaining system performance all together. First, we analyze the privacy level as per user requirement and compute security degree and also encryption algorithms performance. Then, suitable security work is derived by the outcome of analysis and quantified data. Lastly, in different cloud environments the EPPM not only fulfills the user-demand privacy but also maintains the cloud system performance is shown by the simulation results. The EPPM results in 30%-50% when compared to other security methods.

Keywords*:* Cloud Computing, Privacy Protection, Security.

INTRODUCTION

Rain cloud computing is a promising computing style which provides dynamic services, scalable and pay-per-use. The difference between rain cloud computing and other computing models are service-driven, sharing resources, and data hosting in outsourcing storage [1]. Sharing resource makes the hardware management be used more proficient and provides cost-effective benefits for users to reduce the capital cost and additional expenses [2]. Data hosting in outsourcing storage allows rain cloud environment to deliver service quickly to users, and do not expend the waiting time of data transmission required by the services. The major advantages of rain cloud computing is that we can enjoy more convenient services in our daily life.

However, new safety methods are raised at the same time due to the inconsistent system environment. Different with other computing models, there are no explicit users boundaries or perimeters in rain cloud computing. The infrastructure is shared to multi-tenants, and users' data are stored and processed in the sharing resource. While the infrastructure of the sharing resource, store and process users' data that do not owned by them, those data may be revealed or breached by other malicious user in the rain cloud. For this reason, the data privacy protection in rain cloud environment becomes more important than in other cloud computing models. However, the accurate data location in the rain cloud is uncertain so that some existed data protection mechanisms are invalid and also according to presentation or scalability needs data may migrate to different servers. Therefore, as long as the solution of data security is an important concern in the rain cloud.

Author for correspondence:

[1]PG Scholar, Department of Computer Applications, Nandha Engineering College, Erode, Tamil Nadu, India

Email: srajpriyact@gmail.com

[2]Assistant Professor, Department of Computer Applications, Nandha Engineering College, Erode, Tamil Nadu, India

Email: jagadeesan12398@gmail.com

A possible solution for data protection is data encryption. Encryption algorithm offers the advantage of minimum confidence on rain cloud provider [3]. Hence, without limiting to the specific provider users data can migrate from one provider to another provider. Furthermore, encryption algorithm protects data no issue where is its physical location. Regrettably, when performing the encryption algorithm, it frequently consumes a lot of system resources, such as CPU consumption, and stronger algorithm that generates more significant crash to the system production. When applying an encryption algorithm in rain cloud environment, the tradeoff between safety and system presentation become an significant issue. In order to provide the data safety and maintain rain cloud system presentation, Efficient Privacy Protection method (EPPM) is proposed to resolve the problem. According to user-demand privacy requirement and the result of analyzed related information, the EPPM selects an appropriate safety composition that provides enough privacy protection and reduces the extra production operating cost at the same time.

RELATED WORK

Service Models - Rain Cloud

At present, it is existed many different types of rain cloud service models, and three common services models are described as following:

- Software as a Service (SaaS): The applications running on a rain cloud infrastructure provide service to consumer, and it is accessible from various clients through a thin client interface such as a web browser. Some examples - Google Apps (mail, docs, and etc.) and Salesforce.
- Platform as a Service (PaaS): A Specific rain cloud environment can be provided by service provider like some software tools and programming language to consumer for developing, testing, and hosting their applications. The consumer does not control or manage the underlying rain cloud infrastructure in this model. Example- Google App engine.
- Infrastructure as a Service (IaaS): IaaS allows consumer to lease hardware include processors, storages, network, and other fundamental computing resources. In this service model, consumers do not control or manage the original rain cloud infrastructure directly. Consumers control the computing resources through operating systems.

Web Services - Amazon

Amazon is an e-commerce company in the beginning it sells electric business, and now becomes the famous rain cloud services provider that provides web services in IaaS model. Amazon Web Services (AWS) composed by a set of remote computing services offers computing power and storage for users to develop their applications or software [4]. The most central and notable services of AWS are Elastic Compute Rain cloud (EC2) and Simple Storage Service (S3).

In the aspect of safety, AWS provides the protection for

- Virtual Machine (VM),
- physical datacenter and
- network[5].

Network safety issues such as

- Attacks of Distributed Denial of Service,
- Man in the Middle, and
- IP Spoofing

have been protected by AWS. In addition, Xen hypervisor which ensures the isolation of each instance is used for the safety of VM in AWS. The Physical datacenter is protected by using

- video surveillance,
- intrusion detection system, and
- authorized staff for authentication purposes.

AWS provides almost completely protection in authentication and non-repudiation, but the privacy of users' data does not be considered. Thus, the data storing and processing in AWS is insecure, and it becomes an important problem that offers a strong privacy protection for the secrecy of users' data.

In recent years, to resolve the above problem some data protection mechanisms are proposed [6, 7] by applying encryption mechanisms to provide the data secrecy protection. However, they do not take into account the system production impact for their protection mechanism, when their methods are implemented that may cause significant management overhead. [8] discusses the influence of system presentation for data encryption and proposes an

approach for tradeoff between confidentiality and management. Nevertheless, it makes users' data dangerous in sometimes that unveil its content. There is no mechanism to protect the data and considers the presentation overhead at the same time. Thus, we aims to propose a method that secure users' data secrecy in the rain cloud storage and also to maintain the system with minimum overhead.

EFFICIENT PRIVACY PROTECTION METHOD

In this section, we describe a Rain Cloud Data Protection System (RCDPS) that includes the detailed EPPM and its main concepts.

System Architecture

Figure 1 shows the architecture of RCDPS, the top half explains about the selecting protection mechanism which determines a work of encryption algorithm and the division numbers to protect users' data. The bottom half explains data protection flow that data will be protected by implementing system selecting safety composition. The system contains four major components –

- Privacy Analysis,
- Quantification Models,
- Data Division, and
- Data Protection Procedure.

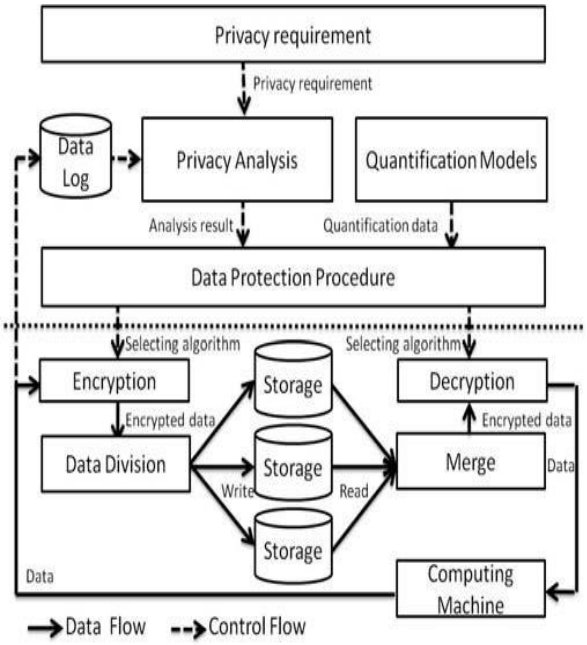

Figure 1. RCDPS architecture

- The privacy analysis in Figure.1 analyzes user-demand confidentiality requirement and collects the update frequency of key which is used to encrypt data.
- The quantification model includes speed aspects and the safety. The safety quantification measures the cracking year of each encryption algorithm used by RCDPS and when executing each encryption algorithm in specific machines the speed quantification measures the mega clock cycles per megabyte.
- The Data Division is an idea using to make data more protected. The analysis result and quantification data are used by Data Protection Procedure.
- The Data Protection Procedure is the kernel function of RCDPS, and it is a main goal in obtaining the composition of encryption algorithm and number of division with maximizing production in satisfied users' privacy requirement.

Privacy Requirement and Analysis

When data is stored in the rain cloud there is no uniform data type. The rain cloud storage has many various data types, like email, video, image, and etc. Based on the sensitive information each data type has different significance degree for the user in the rain cloud. For protecting data secrecy, a safety composition is proposed that consists of an encryption algorithm and the number of data division. Most important data must be protected by strongest safety composition. However, if we used the same strong safety composition to secure data, they would affect the quality of rain cloud services when user requires the unimportant data for the service. Differently, if the weak encryption was used to provide the protection, it would make user's important data timid and can be exposed. Hence the privacy requirements of user's data to do privacy analysis for providing the most appropriate protection have been addressed.

Privacy Level

The privacy level is defined to map users privacy requirement. In the paper, the privacy level is divided into three levels. In our scenario, the levels can be seen as the kinds of speed, hybrid, and security.

Privacy Level 1 (Speed): No sensitive information in the data at this level. The weak encryption composition has been used by users to obtain better performance for using cloud services.

Privacy Level 2 (Hybrid): The requirement of this level presents that data include some sensitive information. If the data uses the weak encryption for protection, users will worry about that the sensitive information is easy to disclose. Nevertheless, users also want to the performance of requiring cloud services not influence too much.

Privacy Level 3 (Security): The data contains most important information can be taken at this level. Users prefer to sacrifice more performance to ensure the confidentiality in order to protect the data security.

Key Update Frequency

The range of safety required by customer is determined by the privacy level after selecting a specific privacy level. The range of each safety $Safety_{range}$ is calculated by

$$Safety_{range} = \frac{Safety\ max}{\| \quad \|}$$

The maximum safety $Safety_{max}$ is the safety score its value is 100. The Plevel is the number of privacy levels we predefined.

The log of data writing is recorded to calculate the times of data written during a recent week, and the update frequency of key is observed by the following equation.

$$Frequency_{KeyUpdate} = \frac{Write_{data}}{A\ period\ \Delta t}$$

When the data is written frequently, the life cycle of key will relatively reduce. Thus the high production safety algorithm will be selected for better I/O management.

Quantification Models

- Safety Quantification - In RCDPS, the security strength of an encryption algorithm is quantified by its cracking year.
- Speed Quantification – CPU consumption can be used to calculate the system performance when an encryption algorithm is performed. Crypto++ is a security simulation tool that evaluates CPU consumption.

Data Division

Some of rain cloud applications are distributed storing the same data in different storages to make the execution more effective in speed aspect, such as MapReduce. In the concept of distributed storage in safety aspect, we consider that implementing the data division after encrypting the data. Main advantage of this method is making data more secure, because the data is encrypted to cipher text and divided into many parts, and the data can be decrypted only by collecting all of division parts. If attackers cannot take any of all division parts by hacked the storing servers, they cannot recover the encrypted data to crack.

Nevertheless, this method is still depending on the degree of users' confidence. The confidence means the users trust to believe that provider cannot disclose their data to attackers. It is similar to the secret sharing, but the secret sharing is not suitable used in

here due to the cost of space that also called as redundancy is too big. We assume that the hacked probability of every storing division server is the same, and the probability of server hacked is H that the value is between 0 and 1. The probability of all of n storing division servers simultaneously hacked is H n . If the data is divided into n +1 division parts and comparing with n division parts, the probability of collecting all division parts is shown as follow.

H n -->H n+1

More division parts make data more safety. Therefore, it can be ensure that by using this method we can enhance data safety, and it can combine with encryption algorithm to offer a safety composition for protecting confidentiality in rain cloud environment.

E. Data Protection Procedure

The main goal of Data Protection Procedure is obtaining the optimal composition of encryption algorithm and number of division by objective function and constraint. The procedure is divided into three phases namely preparation, selection scheme, and data processing.

- Preparation - RCDPS gathers the required parameters of objective function and constraint
- Selection Scheme - To find the composition for expected maximum performance
- Data Processing - The state of data is checked whether it is plaintext or cipher text. Based on the state it have been encrypted or decrypted.

CONCLUSION

In rain cloud environment, we propose an Efficient Privacy Protection Method to secure the secrecy of users data without increasing system production overhead too much. According to different privacy level, our method can examine the related information by using that it has select the most appropriate composition of encryption algorithm and number of data division to afford more secure protection or reduce production overhead. Finally, the proposed scheme satisfies user-demand privacy requirement and offers the better production can be verified by comparing with other safety system are up to 50% and at least 35%.

REFERENCES

[1]. H. Ji and A. Klein, “A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud,” in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, 2009, pp. 735-740.

[2]. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On Technical Security Issues in Cloud Computing,” in Cloud Computing, 2009. CLOUD '09. IEEE International Conference on, 2009, pp. 109-116.

[3]. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, Dec. 2009

[4]. W. Itani, A. Kayssi, and A. Chehab, “Privacy as a Service: PrivacyAware Data Storage and Processing in Cloud Computing Architectures,” in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, 2009, pp. 711-716.

[5]. V. D. Cunsolo, S. Distefano, A. Puliafito, and M. Scarpa, “Achieving Information Security in Network Computing Systems,” in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, 2009, pp. 71-77.

[6]. R. Prabhakar, S. Seung Woo, C. Patrick, S. H. K. Narayanan, and M. Kandemir, “Securing Disk-Resident Data through Application Level Encryption,” in Security in Storage Workshop, 2007. SISW '07. Fourth International IEEE, 2007, pp. 46-57.

[7]. Arjen K. Lenstra and Eric R. Verheul, “Selecting Cryptographic Key Sizes,” Journal of Cryptology, vol. 14, pp. 255-293, 1999

[8]. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. “Xen and the art of virtualization,” In Proceedings of the Symposium on Operating Systems Principles (SOSP), Oct. 2003.

[9]. Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey, and Jinjun Chen, Member, IEEE,”A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving,” IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013

[10]. Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage,” IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013

[11]. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou,Department of ECE," Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data," IEEE Transactions On Parallel And Distributed Cloud Computing Systems,Volume:25,Issue:1,Issue Date:Jan.2014

[12]. Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE," Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions On Computers, Vol. 62, No. 2, February 2013

[13]. Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE," Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," IEEE Transactions On Parallel An Distributed Systems, Vol. 26, No. 1, January 2015