Computer Science • 15 (1) 2014 http://dx.doi.org/10.7494/csci.2014.15.1.3

Mariusz Kapanowski
Renata Słota
Jacek Kitowski

RESOURCE STORAGE MANAGEMENT MODEL FOR ENSURING QUALITY OF SERVICE IN THE CLOUD ARCHIVE SYSTEMS

Abstract *Nowadays, service providers offer a lot of IT services in the public or private cloud. Clients can buy various kinds of services, such as SaaS, PaaS, etc. Recently, Backup as a Service (BaaS), a variety of SaaS, was introduced there. At the moment, there are several different BaaS's available to archive data in the cloud, but they provide only a basic level of service quality. In this paper, we propose a model which ensures QoS for BaaS and some methods for management of storage resources aimed at achieving the required SLA. This model introduces a set of parameters responsible for an SLA level which can be offered at the basic or higher level of quality. The storage systems (typically HSM), which are distributed between several Data Centers, are built based on disk arrays, VTL's, and tape libraries. The RSMM model does not assume bandwidth reservation or control, but rather is focused on management of storage resources.*

Keywords storage, backup, cloud, management, QoS, SLA

1. Introduction

The globalization of scientific research and the great importance of data are now the most important factors in the computational science paradigms. e-Science [3], the Fourth Paradigm [4] and data farming computing [6, 7, 8, 9, 10] – name only a few – are the domains in which data-related problems are focal points of interest, requesting the efficient organization of data storage and data access. On the other hand, the collaboration of scientific groups and requirements for easy-to-use computational resources, together with the neglect of problems of ownership of IT infrastructure, result in the increasing popularity of the cloud paradigm [5], offering the user the required services. Many types of cloud environments do exist nowadays, like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) with many kinds of technical realizations, but the data problems brought Backup as a Service (BaaS) on, with great interest concerning the architecture at the issues and use cases of such BaaS cloud environments. In spite of the fact that BaaS clouds do exist currently, they address neither the problems of Service Level Agreement nor any Quality of Service (QoS) management [11, 12].

In this paper, a management model of storage resources for QoS ensurance in cloud systems is presented. The model is based on our previous study [1, 2] as well as on some practical experience gained during the implementation of commercial backup systems.

This paper is organized as follows: the state-of-the-art section that includes a review of commercial BaaS services available on the market (including the software dedicated for BaaS and Service Providers) and an example of distributed archive system developed for scientific purposes. Section 3 addresses a resource storage management model, described in full detail regarding the parameters tackled in the paper, QoS levels, and management policies. The next section provides a detailed description of management policies and actions related to ensuring higher QoS in the cloud backup and archive systems. Section 5 is dedicated to the management of the distributed storage systems in order to obtain a higher QoS. The planned implementation, tests, and conclusion are presented in Section 6. The last section refers to future work related to developing the model.

2. State-of-the-art (related works)

A backup is a copy of data intended for restoring the original after a data loss event. BaaS services available on the market offer different types of services in the field of backup and archive data. Customers require the availability of backup with a lot of different data from BaaS services: files from various file systems and with many of extensions, data bases (table, logs, settings), application data and settings, i.e., MS Exchange server (on the message or mailbox level), etc. Currently, there are numerous cloud backup services available on the market. In this section, we present three different commercial BaaS: Mozy [13], iBard24 [14], and msejf [15] while describing

the scope of services offered by each of them. As an example of the software used to provide BaaS, Asigra [16] and NDS [16] are presented. The review in this section includes functional aspects of available BaaS because nowadays, service providers offer BaaS without a choice quality of service level. All services are offered on the same level – usually the best effort of quality.

Mozy is one of the BaaS services which is backed by VMware and the EMC Corporation. There are three levels of services offered by Mozy: Home, Pro, and Enterprise. Customers can perform the backup of data, which can be: simple files or system files, shared files from NAS systems, databases and applications such as MS SQL, MS Exchange, MS SharePoint (with their settings), according to the required level of service.

iBard24 and msejf are two of the most popular BaaS systems on the market in Poland. The iBard24 system was created by Comarch S.A. and offers two kinds of accounts: Standard and Premium. The Standard account is dedicated to individual customers and allows for the backup of data coming from user applications (photos, audios and pst files) and office data (documents). The second level (Premium account) is dedicated to business customers and allows for an extended backup of data starting with files, folders up to MS SQL databases from personal computers, laptops, and servers. Backup of data from CIFS/FTP shared resources and archive e-mails is also possible. iBard complements its service with the backup of an ERP application made by Comarch. The predefined retention policy of iBard BaaS allows users to keep up to twenty versions of the same file.

Another Polish service provider – Komputronik S.A. – offers its BaaS service named "msejf". This BaaS service includes three levels of services: 10 GB, Unlimited, and PRO. The first and second examples are dedicated to home users while the third one is aimed at small or medium businesses. The supported operating systems are limited only to Windows (XP, Vista, and Win7). No support for server systems seems to be a big disadvantage.

Asigra [16] is one of the available software solutions which can be used to build backup cloud services. This software is dedicated to private or public clouds for BaaS building. Asigra allows service providers to store backup and archive data on their own Data Center resources or on other public clouds by providing appropriate interfaces for: Amazon S3, EMC Atmos, and Mezeo MCSP. The products powered by Asigra can be used for backup servers, databases, applications, laptops and desktops, and mobile devices such as tablets and smart phones. Although Asigra allows for building backup and archive services, it doesn't support QoS provisioning.

This year, the Sejf Danych (Data Safe) service [17] was introduced – the first BaaS service on the Polish market that is powered by Asigra. The Sejf Danych offers cloud-oriented data backup to a number of Data Centers in Poland (e.g., S3, Sinersio, EXEA, etc.) with replication of data to geographically-separate Data Centers. All of the backup data is encrypted during transferring and when stored. The de-duplication of backup data is enabled on the client's demand. This service – Sejf Danych – protects not only files but the whole operating system a well. Sejf Danych also offers Disaster

Recovery features like Local or Remote VDR (Virtual Disaster Recovery). The client could very quickly start up (locally or in the service provider's Data Center) the whole server (as a virtual machine) from the backup. It ensures business continuity for clients of the service.

A second example of software which can provide backup and archive services is the National Data Storage system (NDS) [18, 19, 20, 21, 22, 23, 24], developed at the CYFRONET Academic Computer Center. The NDS is a distributed data storage system intended to provide backup, archiving, and data access services. These services ensure a high level of data protection by using replication techniques. Based on this software, the Platon U4 service is offered. Platon U4 is a common backup service targeted towards the scientific community of Poland. This service provides a reliable and highly-available data storage as well as easy, efficient, and universal access. Users can use standard protocols, including SFTP and WebDAV. This enables easy integration of the system with popular tools (e.g., WinSCP, OS built-in WebDAV clients). For efficient transfers of large data volumes, the GridFTP protocol can be used to enable high-performance parallel transmission, even on long-haul links. High availability is also obtained by multiple redundant components and transparent data and meta-data replication. This service provides high storage safety and security due to the support for end-to-end data encryption, data integrity control, SSL-protected data transmission, and security procedures employed at storage sites.

In its final version, the NDS2 project will implement support for QoS and SLA functionalities. The following QoS functionalities are addressed in NDS2 system – the user can choose:

- a minimal data transfer rate, which is satisfactory to them,
- a data protection level,
- a data availability level.

The service responsible for QoS in the NDS2 is still under development.

As mentioned above, the commercial BaaS clouds do currently exist, but they address neither the issues of Service Level Agreement nor any Quality of Service (QoS) provisioning. However, some of the cloud backup services (i.e., NDS2) attempt to resolve the issues of QoS, but meet them to a limited extent. NDS2 addresses the QoS provisioning issue, but it isn't available yet. Our paper is aimed at addressing the possibility of QoS provisioning in the cloud backup and/or archive services.

3. Resource Storage Management Model

The goal of our research is to build a high-level and universal management model for controlling storage resources in the cloud backup and archive services to attain QoS provisioning. The result of this work is Resource Storage Management Model (RSMM). RSMM consists of three main components: parameters, QoS levels, and management policies, which are discussed in the rest of this section.

3.1. Parameters

Four parameters have been defined in the Resource Storage Management Model – they are:

1. Performance
2. System Load
3. High Availability
4. Security

The above parameters used in the RSMM model have been chosen based on the most important factors indicated by customers in a questionnaire. A diagram of the parameters used in the RSMM model are shown in Figure 1. As one can see, these parameters are placed in the coordinate system, because obtaining a required level for one of them sacrifices achieving the assumed level for another one. For example, obtaining high performance parameters sacrifices keeping a low level load of the storage system, and providing many replicas sacrifices high security, because an encryption key can be easier broken by increasing the number of replicas.

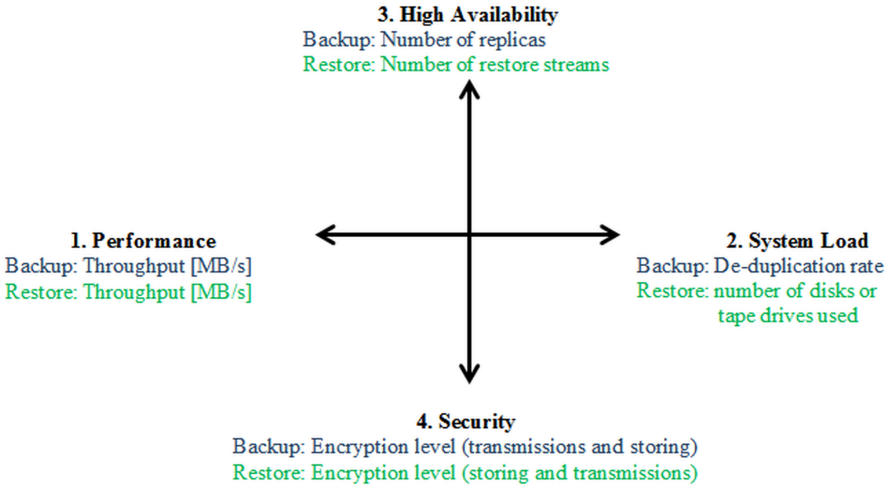

Figure 1. Diagram of RSMM model parameters.

Each component (parameters, QoS levels, and management policies) of the RSMM model is developed for two use-cases: backup and restore. The parameters (the first component) are expressed in variable units for these two use-cases (see Fig. 1). For the backup use-case, Performance is presented as a throughput in MB/s, System load as a de-duplication rate, High Availability as a number of replicas of a file, and Security as a data encryption level (for a backup transmissions and storing of data). For the restore use-case, the units of the Performance and Security parameters are the same as before. But the High Availability parameter means the number of restore streams which are used in parallel during the restore procedure of a file. The

System Load parameter has also a different unit for restore use-case and is presented as a number of disks or tape drives used.

The Performance parameter has the same units for both use-cases, but could have a different value. For example, the throughput could be on the level of 5 MB/s for the backup of user data and 100 MB/s for restoring the same data. The same situation is for the Security parameter; i.e., data could be encrypted with algorithm AES-256 for backup, and the same data can be restored only with password to a user account.

3.2. QoS levels

The RSMM model introduces a concept of services with different Quality of Service (QoS) levels. The Quality of Service is determined based on sets of parameters and the levels of their values. Two examples of the service quality levels for the backup use-case are presented in Figure 2. The first one is "base QoS level" for the lowest service quality. The values of parameters included in the sets are on the lowest level and, additionally, are not ensured (i.e. up to xx MBs only). The value of Performance is only up to 10 MB/s, System Load is on the highest level – there is no de-duplication. The real High Availability doesn't exist – without of replicas, all files are stored only as single original files. And Security relies only on a password to the user's account – there is no data encryption.

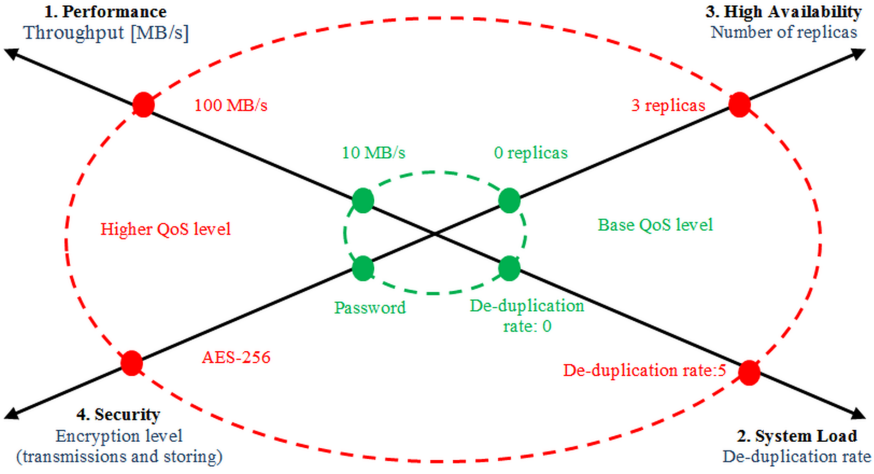

Figure 2. Diagram of QoS concept.

The second QoS level is presented as a "higher QoS level". The value of Performance is ensured on the level of 100 MB/s, and System Load is kept on a higher level of de-duplication rate: 5. High Availability offers three replicas of original files, and Security ensures data encryption of transmission and storage of data with the AES-256 bit key.

Note that the sets of parameters include only points on an axis, and a ring is intended only for grouping them. The values of the parameters are not continuous but rather discrete. In an additional service, a mix mode can be offered – some parameters on the "base QoS level" and the rest on the "higher QoS level".

All of the parameters on the base and higher level of quality were complemented by a third dimension – the cost factor. The projection of costs on the axis is shown in Figure 3.

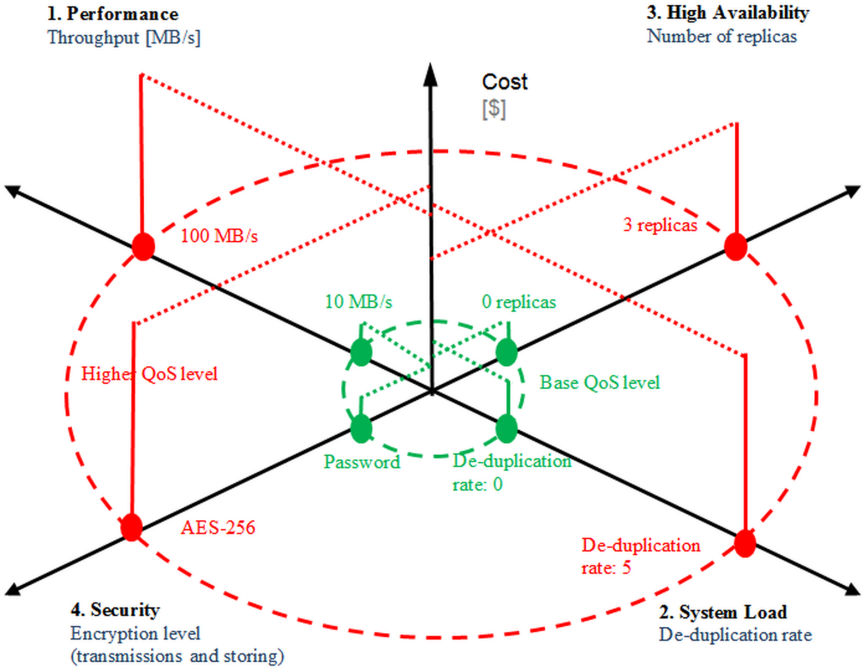

Figure 3. QoS Diagram with cost factor.

The total cost of the service on the "base QoS level" is a sum of the costs of four parameters (Performance, System Load, High Availability, and Security) with values at the lowest quality level (not ensured). The total cost of the service at the "higher QoS level" is usually higher than that at the "base QoS level". This cost is not specified by the model, because it strongly depends on the kinds of hardware and software used in the cloud storage systems.

3.3. Management policies

The management policies are the third component of RSMM; they are different for each of the model parameters (Performance, System Load, High Availability, Security); additionally, they have the backup and restore use-cases as a third dimension. Each management policy has a set of actions associated with the storage of data to

obtain a required level of service quality. More details about the management policies are given in Section 4.

4. Definitions of RSMM management policies

To obtain the required QoS level, we introduce the resource management that now consists of three management policies: Proactive – based on resource reservation; Interactive – making use of service prioritization; and Best Effort. These policies are dedicated to services with higher SLA level, excluding the Best Effort policy (which handles only services on the base QoS level). Each of these policies is defined separately for each parameter and for two of the use-cases: backup and restore.

4.1. Policy for the Performance parameter

All of the policies and actions associated with the Performance parameter are collected in Table 1.

Table 1
Policies and actions associated with the Performance parameter.

Policy type and Use–Case	**Backup**	**Restore**
Proactive	Reservation of disk space i.e.: x TB on SSD disks	Data stores on disks i.e.: moving data T2D
Interactive	Staging i.e.: moving data D2T	Analysis of the state of the system, and selection of "the best-copy/replica"
Best Effort	The lowest quality, insufficient resource – jobs are rejected	The lowest quality, insufficient resource – jobs are rejected

Each of these policies includes a set of actions to enforce the assumed level of service quality. For example, for the Performance parameter and for the backup case, the Proactive policy enforces reserving the required disk space on Solid State Disks featuring very high performance. The Interactive policy includes a staging action for moving data from disk resources to tape carriers. The last type of policy – Best Effort – checks the available resources, and based on that, backup jobs are limited or rejected. For the restore case, the Proactive policy moves data from tape to disks to obtain better throughput. The replica selection using system analysis and the diversification of user requests for the same policies are implemented internally in the Interactive policy. The Best Effort policy for the restore use-case checks the available resources similarly as for backup, and could reject restore jobs under critical conditions.

4.2. Policy for the System Load parameter

All of the policies and actions associated with the System Load parameter have been collected in Table 2.

Table 2
Policies and actions associated with a System Load parameter.

Policy type and Use–Case	**Backup**	**Restore**
Proactive	De-duplication 'post process'	Unde-duplication in the background
Interactive	De-duplication 'in-line'	Analysis of the state of the system, and selection of the least loaded system
Best Effort	No de-duplication	The lowest priority, Insufficient resource – no restore

For the System Load parameter and for the backup case, the Proactive policy enforces de-duplication of the data that has already been stored – a postprocess de-duplication regarding the data that has been already backed up. The Interactive policy includes de-duplication performed in-line (during the backup process). The data is stored without any de-duplication internally in the Best Effort policy, and it consumes the most resources. For the restore case, the Proactive policy reverses the de-duplication process of data in the background in order to obtain the data ready for restore. The replica selection by the system analysis and the diversification of user requests for the same policies are implemented internally in the Interactive policy. The highest priority for the System Load parameter is given to the replica selection from the lowest system load. In the restore use-case, the Best Effort policy rejects jobs with the lowest priority if other services (with higher QoS levels) consume all the resources.

4.3. Policy for the High Availability parameter

All of the policies and actions associated with High Available parameter have been collected in Table 3. For the High Availability parameter and for the backup case – the load balancing between storage nodes with making use of RAID systems, on-line synchronous replication and no replica at the lowest level for Proactive, Interactive and Best Effort policies are used. Whereas for the recovery case – the number of requested replicas supported with asynchronous replication, best replica selection supported by parallel recovery and restore from the original file according to the least system influence are defined.

Table 3
Policies and actions associated with the High Availability parameter.

Policy type and Use–Case	**Backup**	**Restore**
Proactive	Storage Nodes load balancing, RAID level	Asynchronous replication
Interactive	Synchronous replication (during backup)	Analysis of the state of the system, and selection of 'the best copy/replic', or parallel recovery
Best Effort	No replica	Only the original file – no replica

4.4. Policy for the Security parameter

All of the policies and actions associated with Security parameter are collected in Table 4.

Table 4
Policies and actions associated with the Security parameter.

Policy type and Use–Case	**Backup**	**Restore**
Proactive	Encryption of transmission i.e.: AES 128/256	Encryption of stored data (disk array/tape library)
Interactive	Encryption of stored data (disk array/tape library)	Encryption of transmission i.e.: AES 128/256
Best Effort	Minimum security level: Password	Minimum security level: Password

For example, for the Security parameter and for the backup case, the Proactive policy ensures encryption of transmission between source systems and cloud storage, and the interactive policy encrypts the stored data. The encryption is based on the AES algorithm with up to a 256-bit encryption key. For the restore use-case, the Proactive and Interactive policies are swapped compared with the backup use-case. The last type of policies for both use-cases – the Best Effort – provides only the password to the user account – there is no data encryption.

5. Cloud archive systems architecture

A typical storage system architecture underlying BaaS is shown in Figure 4.

Customers are enabled to access BaaS service in the cloud, but their data sent to this cloud is managed only by the Service Provider. In the typical distributed or

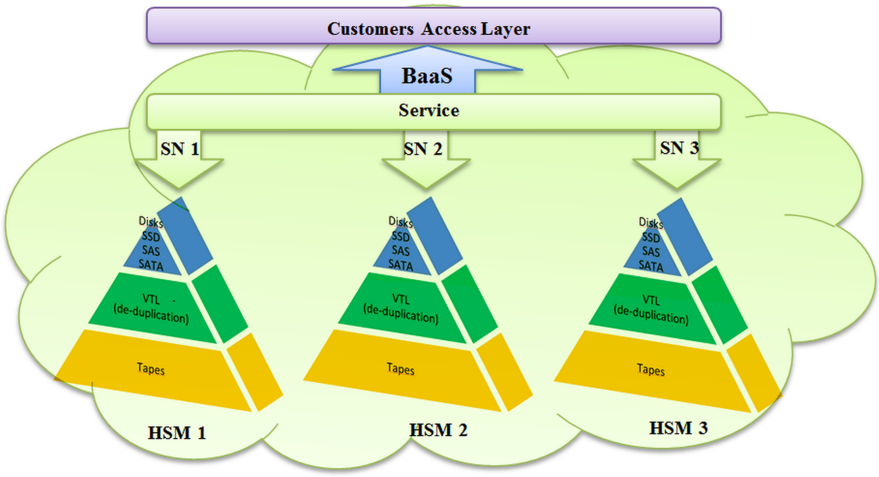

Figure 4. Distributed and hierarchical storage systems in BaaS.

clouds storage environments like in Figure 4, there are many kinds of hardware, like: disks array, tape libraries, and virtual tape libraries (VTL). The disk arrays include different types of disks (SSD, SAS, NL-SAS, SATA) with different performance levels (SSD and SATA disks have the highest or the lowest performance, accordingly). But a problem regarding disks for backup storage still relates to the cost. The price of a SSD disk is very high vs. the low capacity. Disks with higher capacity (SATA, NL-SAS) are still more expensive than tapes, while disks need a power supply and constant cooling, so they produce an additional cost of maintenance. The VTL is another type of disk space for backup, and in contrast to the traditional disk array, it offers the de-duplication feature and tape libraries logic (virtual robotic, virtual tapes and drivers). Service Providers could store much more data based on VTL (using de-duplication) and additionally on the disks, so performance is consistently high. The costs of VTL (especially with the de-duplication feature) are still high, but they save space by de-duplication and the savings due to the license are re-compensated. The last type of storage to mention is a tape library, which can store a vast amount of backup data. Currently, LTO-6 technology offers 2,5 TB native data capacity per cartridge. So now, it is possible to store large sets of data on a long term carrier for a long time and at a relatively-good price.

In the distributed or clouds storage environments, these three kinds of hardware are grouped into HSM (Hierarchical Storage Manager) represented as Storage Nodes as shown in Figure 4. An HSM includes disk arrays, VTL, and tape libraries. Sometimes, HSM is reduced and has only two storage layers, and in extreme conditions, only one (i.e., disk array only). The architecture with SN and HSM enabling the storage of data on different carriers and in different locations provides high performance and high availability of data for minimal costs.

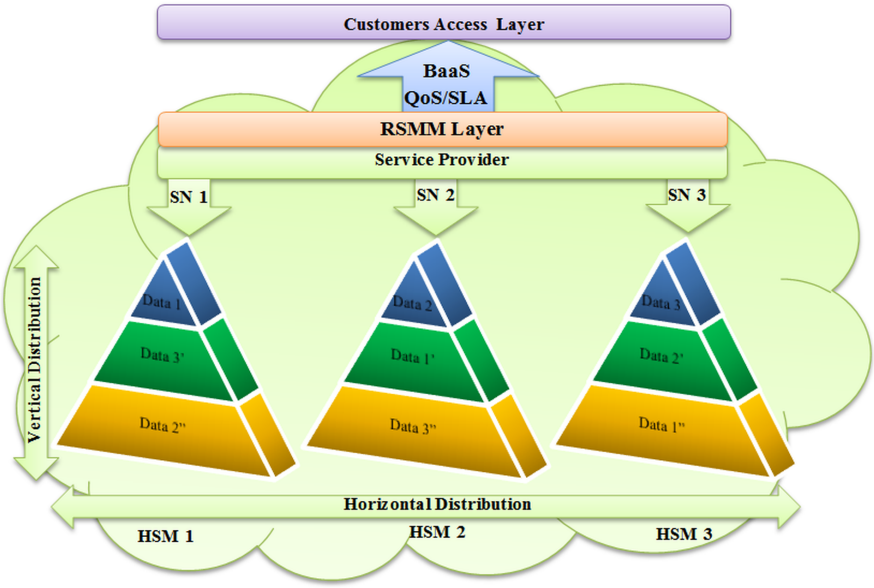

Figure 5. Vertical and horizontal distributions of data for QoS/SLA purpose.

One of the examples of storage and data management is migration of data between SN and a layer in the HSM. Service Providers migrate data between fast, small-capacity disks and slow, large-capacity tapes (Vertical Distribution). Due to the HSM features, Service Providers can offer storage of big data sets with acceptable performance and at a good price. To ensure High Availability and increase the capability of restore operations, Service Providers distribute data between geographically-distant sites (Horizontal Distribution). Example of this data management is shown in Figure 5.

6. Decision maker (QoS Broker)

The BaaS service provider stores all of the backup data from end users. Based on the management policies implemented by the service provider, the backup data is distributed across different storage layers and in different sites.

The RSMM model uses a set of actions in order to enforce the required operation previously defined for each of the management policies. These actions are executed by the QoS Broker module, which directly cooperates with the backup software and storage resources as is shown in Figure 6. The QoS Broker as an executive module is one of the most important parts of RSMM, because it has to make decisions to ensure higher QoS. Good decision making and proper data management by the QoS Broker is the crucial question in providing a higher QoS by the backup service. In order to support QoS Broker's functionality in making decisions, we propose using

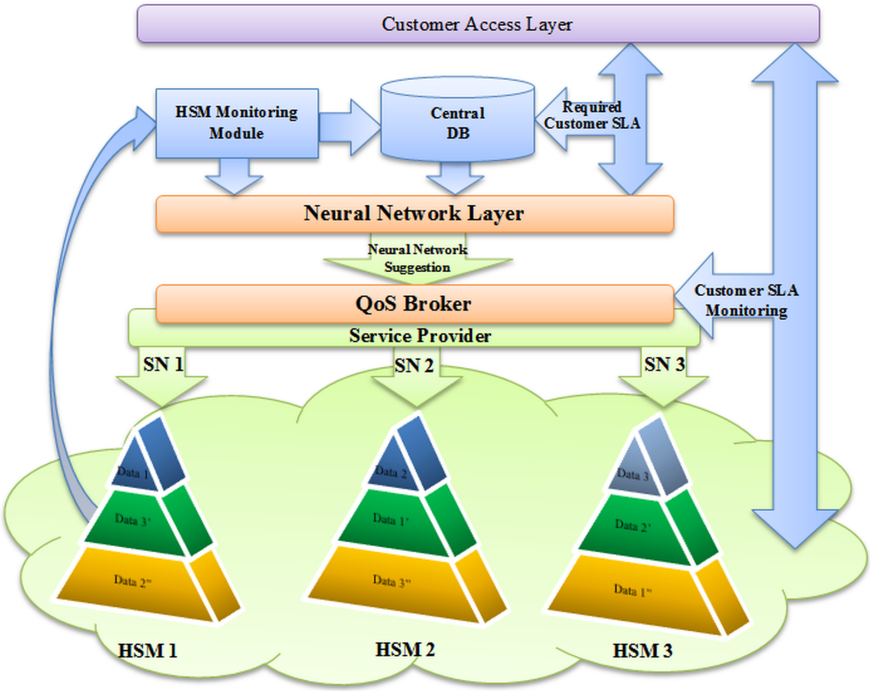

Figure 6. Data management with QoS Broker supported by neural network.

a neural network in the RSMM model. The input data to the neural network is the data coming from the:

- customer SLA,
- database data, which collects the values of all HSM (or storage systems) parameters' (static and dynamic),
- HSM monitoring module, which monitors state of the storage systems.

This database is the central component of knowledge about the cloud storage environment states, and the neural network helps QoS Broker make decisions based on this data. Static values are inserted into the database during RSMM implementation and configuration, while dynamic values are updated at fixed time intervals by the HSM monitoring system. The customer's SLA requirements are merged with the database data that constitutes input data to the neural network. This neural network, which is only an "advisor body", helps QoS Broker to make decisions regarding which action should be taken to obtain the required level of service quality.

The current fulfillment of SLA is obtained from the customer SLA monitor (not to be confused with the HSM monitoring module) – compared to the required SLA level contained in the contract. If the SLA level is not met, QoS Broker has to undertake an action which meets it. However, it is most probable that a single action won't meet

SLA requirements, so this process has to be iterative. If the level of SLA is not met after 10 or so actions, the QoS Broker sends an error message to the administrator for future investigation.

7. Conclusions

In this paper, we introduced an RSMM model that consists of three main components: parameters, QoS levels, and management policies. A set of actions concerning Proactive, Interactive, and Best Effort management policies for the tackled parameters (Performance, System Load, High Availability, Security) has been defined. Additionally, each parameter was considered in two use-cases: backup and recovery. Taking into account the architecture of BaaS built based on HSM systems, we proposed managing data by using a QoS Broker supported by neural network. At this point, it is worth recalling that the RSMM model is general-purpose one. The RSMM model and QoS Broker are both generic; hence, they could be used in any distributed-data environment. In previous projects like the NDS, only a simplified version of QoS levels was presented. All of the management policies with actions were limited [1] and the parameters were limited as well [2]. But in this model, QoS Broker using heuristic tools supported by a neural network brings a wider range of possibilities to using and attaining higher SLA levels.

Future work on the implementation of the RSMM model will be focused on the QoS Broker and the feedback loop of SLA parameters. The intelligence of the RSMM model is ensured by the use of a neural network and influencing QoS Broker decision-making that arises from SLA parameters.

Acknowledgements

This work is supported by AGH-UST grant No. 11.11.230.015.

References

[1] Słota R., Nikolow D., Polak S., Kuta M., Kapanowski M., Skałkowski K., Pogoda M., Kitowski J.: Prediction and Load Balancing System for Distributed Storage. *Scalable Computing Practice and Experience, Special Issue: Grid and Cloud Computing and their Application* 11(2): 121–130, 2010, ISSN 1895-1767.

[2] Słota R., Nikolow D., Kuta M., Kapanowski M., Skałkowski K., Pogoda M., Kitowski J.: Replica Management for National Data Storage, In: R. Wyrzykowski, J. Dongarra, K. Karczewski, J. Wasniewski (Eds.), *Proceedings of Parallel Processing and Applied Mathematics – PPAM 2009, 8th International Conference*, Wroclaw, Poland, September 2009, LNCS 6068, vol. II, Springer 2010, pp. 184–193.

[3] Hey T., Trefethen A. E.: Cyberinfrastructure for e-Science. *Science* 308(5723): 817–821, 2005.

[4] Hey T., Tansly S., Tolle K. (Eds.): *The Fourth Paradigm: Data-Intensive Scientific Discovery*. Microsoft Research, October 2009.

[5] Mell P., Grance T.: *Effectively and securely using the cloud computing paradigm*. National Institute of Standards and Technology. October 7, 2009.

[6] Kryza B., Król D., Wrzeszcz M., Dutka L., Kitowski J.: *Interactive Cloud Data Farming Environment For Military Mission Planning Support*, *Computer Science* 13(3): 89–100, 2012.

[7] Brandstein A., Horne G.: *Data farming: A meta-technique for research in the 21st century*. In: Maneuver Warfare Science 1998. Marine Corps Combat Development Command Publication, 1998.

[8] Choo C. S., Ng E. C., Ang C. K., Chua C. L.: Systematic data farming – an application to a military scenario. In: *Proc. of Army Science Conference*, 2006.

[9] Forsyth A., Horne G., Upton S.: *Marine corps applicatons of data farming*. In Kuhl M. E., Steiger N. M., Armstrong F. B., Joines J. A. (Eds.), *Proc. of the 2005 Winter Simulation Conference*, pp. 1077–1081, 2005.

[10] Horne G., Meyer T.: Data farming: Discovering surprise. In Ingalls R. G., Rossetti M. D., Smith J. S., Peters B. A. (Eds.), *Proceedings of the 2004 Winter Simulation Conference*, pp. 1082–1087, 2004.

[11] Slota R., Nikolow D., Skałkowski K., Kitowski J.: Management of Data Access with Quality of Service in PL-GRID Environment. *Computing and Informatics* 31(2): 463–479, 2012.

[12] Nikolow D., Słota R., Lakovic D., Winiarczyk P., Pogoda M., Kitowski J.: Management methods in sla-aware distributed storage systems, *Computer Science* 13(3): 35–44, 2012.

[13] Mozy, `http://mozy.com` (last access 30th of June 2013)

[14] iBard, `http://www.ibard24.com/products/ibard24-backup-online` (last access 30th of June 2013)

[15] Msejf, `http://www.msejf.pl` (last access 30th of April 2013)

[16] Asigra, `http://www.asigra.com` (last access 30th of June 2013)

[17] Sejf Danych `http://www.sejfdanych.pl` (last access 30th of June 2013)

[18] National Data Storage project, `http://nds.psnc.pl` (last access 10 January, 2013).

[19] Nikolow D., Słota R., Polak S., Mitera D., Pogoda M., Winiarczyk P., Kitowski J.: Model of QoS Management in a Distributed Data Sharing and Archiving System. *International Conference on Computational Science*, ICCS 2013, Procedia Computer Science, vol. 18, 2013, pp. 100–109.

[20] Słota R., Król D., Skałkowski K., Orzechowski M., Nikolow D., Kryza B., Wrzeszcz M., Kitowski M.: A Toolkit for Storage QoS Provisioning for Data-Intensive Applications, *Computer Science*, 13(1): 63–73, 2013.

[21] Funika W., Szura F.: Data Storage Management Using AI Methods, *Computer Science*, 14(2): 177–190, 2013.

[22] Król D., Funika W., Słota R., Kitowski J.: SLA-Oriented Semi-Automatic Management of Data Storage and Applications in Distributed Environments, *Computer Science*, 11: 37–50, 2010.

[23] Nikolow D., Słota R., Kitowski J.: Grid Services for HSM Systems Monitoring, In: R. Wyrzykowski, J. Dongarra, K. Karczewski, J. Wasniewski (Eds.), *Proc. of 7-th International Conference, PPAM 2007*, Gdansk, Poland, Septem-ber 2007, LNCS 4967, Springer 2008, pp. 321–330.

[24] Dutka L., Kitowski J.: *Stochastic Approach for Secondary Storage Data Access Cost*, In: P. M. A. Sloot, A. G. Hoekstra, T. Priol, A. Reinefeld, M. Bubak (Eds.), *Proc. of Advances in Grid Computing – EGC 2005 European Grid Conference*, Amsterdam, The Netherlands, February 14–16, 2005, Lecture Notes in Computer Science, no. 3470, Springer, 2005, pp. 796–804.

Affiliations

Mariusz Kapanowski
AGH University of Science and Technology, Krakow, Poland, mkapanow@agh.edu.pl

Renata Słota
AGH University of Science and Technology, Krakow, Poland, rena@agh.edu.pl

Jacek Kitowski
AGH University of Science and Technology, Krakow, Poland, kito@agh.edu.pl

Received: 3.09.2013
Revised: 19.09.2013
Accepted: 20.12.2013