Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-31

THE METHODOLOGY FOR IMPLEMENTATION OF CLOUD COMPUTING IN THE ENTERPRISE AND UNIVERSITIES

[Zuzana Prišťáková, Ivana Rábová]

***Abstract*—This article analyzes the process of the implementation of cloud computing in a university environment. The goal of the implementation is to enhance the security of the data, that are handled via cloud. Two different implementation environments to increase the accuracy of the data are used – the enterprise and the university environment. The verification of the formalized methodics contains the architecture proposal, the infrastructure and implementation proposal, and testing of the virtualized technologies. The undertaken research had aim to identify the life cycle of the data, that are stored in the virtualized environment (where the observed constituents are the implementation environment requirements, the origin of the data, the data sensitivity, the integrity preservation and secrecy of the data, and the linking between the virtualized environment and hardware). As generalized methodics, there we can find the available algorithms, standards, and security protocols which are recommended by the security organisations.**

Keywords— cloud computing, data security, data integrity

I. Introduction

Storing data in the cloud can be considered quite attractive, outsourcing focusing on daily data management [1]. Provider cloud services, some basic best practices for the safe use storing data in the cloud, as well as methods and standards for monitoring data integrity without regardless of data storage [2].

To achieve greater security and compliance data redundancy, data are stored together in the cloud and locally [3]. One of the main advantages of storing data in the cloud is unlimited access to these data, and comprises the unlimited time and access points. For such firms are worth to enter the cloud-based solutions and minimize the load physical storage devices, used at the same computer and multiple devices to access data in real time (real-time reporting) [2].

In this case, in the manufacturing of storage cloud think about the specialization repository. Even though there are hundreds of cloud storage, each storage is oriented to other requirements, such as storing communication through e-mail, storing profiles of employees storing project documentation, etc. [2]. Of course, requirement can also store all type of documents.

Zuzana Prišťáková
Mendel University in Brno
Czech Republic

II. Implementation of cloud computing in corporate and university environment

Cloud technology is used in a variety of work environments. Cloud computing provides a highly scalable, so its use as a repository can be a performed in any environment using available information technologies. From the characteristics of the cloud it shows that one can use data storage several users. A user on the Internet can communicate with many servers at the same time and these servers sharing information [4].

Sharing real-time information provides the users improve work efficiency. Today's cloud platform, such as Microsoft and Google will provide free services to students and employees in educational institutions, including email, contact lists, calendars, document storage, creating and sharing documents and the ability to create web pages [5]. However, services cloud computing can provide a separate university with the possibility to continue benefit from new developments in IT technologies at an affordable cost.

In the future, it is highly likely that cloud will become the baseline technology for small and medium-sized enterprises and educational institutions [6]. British National Computer Centre (NCC) estimates that SMEs can reduce the total cost of ownership of technology using a hosted solution [7]. Nabil (Nabil, 2010) states, that university management should identify and use new technologies that are cost effective, and thus seek the widest possible and equitable access to technology for students and staff.

A. A baseline study in the university

Use of cloud computing in university constitutes is 4 percent of total use cloud in other sectors (the largest use is in the area of financial services and management) [8]. Scalable cloud-based intelligent infrastructure It is a sensible solution for utilities, smart data centers everywhere being present computer technology, automation, virtualization and network [9]

Students at university use various Internet options, e.g. share documents, videos, presentations, software, communication through email, alerting and so on [10]. Betsy and Praveen [11] presented a comprehensive introduction to use the cloud at universities. Delic and Riley [12] evaluated the current status of educational institutions as the need to transform infrastructure global, reliable and effective, and through the use of cloud computing. Educational institutions and universities always require upgrading its software and IT hardware, thus to attract students and keep pace with rapid developments in the field information technology.

Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-31

B. *Tuncay model of university infrastructure cloud*

Tuncay created a model, which seeks to meet the needs administrative staff (student affairs, finance and accounting, purchasing and procurement) and education, training and research in the context, the needs of students and academics, particularly in education institutions. This model is based on cloud infrastructure, which was divided block: user, network storage, virtualization, processor, storage, business continuity and firewall.

From the student perspective, a model is constructed so that it does not restrict or objects schools, and the content is dynamically changed periodically. user cloud In this case, coupling with commercial services of third parties to create new applications [7].

Platform planned under the cloud provides that the content of the application is before the Applications themselves in the center [13]. Cloud content (scientific and social subjects, arts, opinions, textbooks, encyclopedias) is controlled by service providers and users is available whenever request it [7].

The improved data mining techniques used filter that is required content to help students. The objective is student work full access courses or schools, and should therefore be dynamically changed existing content and at certain intervals [7]. Custom services are combined with commercial third-party services to create new applications [7].

III. Results

A. *Safety rules*

Safety rules are based on the fulfillment of the primary functional requirements the model, and it is storing data in the cloud. Data storage brings an end user. Data can only be imposed on the site end user. Login is repeating operation, subject to control credentials. After connection sends client demand for data storage, this is handled by a chronological compliance with these safety rules:

Rule 1. Identify the input data - based on the input data class system determine what data to save. (manager lifecycle data)

Rule 2. Require encrypted data - the determination of input data is needed require encrypted data. (end-user directory)

Rule 3. Identify data security - data is to be attributed to each allowed data security due to their sensitivity. Based on security permissions it is assigned a level of data security. (manager lifecycle data file administrator classified data)

Rule 4. Set the minimum privileges - privileges are minimal extension enabling security data. Minimum privileges determine what the minimum operations are permitted for the implementation of data while operations will not cause data leakage or new risks. (manager lifecycle data file)

Rule 5. Encrypt data - based on the previous steps 3 and 4 encrypted data. (manager lifecycle data directory)

Rule 6. Label data - to maintain the integrity of data is data attributed code (hash value), the label data consists of the following steps. (manager data life cycle, risk manager, file)

Rule 7. Identify the risks - for flagging data is needed to determine the risk procedures, which they can be carried out with the data and could result in theft or complete loss of data. (risk manager, administrator of classified data)

Rule 8. Create Security Policy - the identification of the hazards shall be drawn up safety policy that points to the way of dealing with risk procedures and method their prevention. (risk manager)

Rule 9. designate border protection - protection threshold data compiled on the basis identified risks and security policy (list manager communications)

Rule 10. Ensure data - secure data is encrypted and has assigned code. Secure data contain a defined risk, security policy and boundary data protection. (directory)

Rule 11. Create a security type - Secure data are assigned security type, inclusion in the security level under level data contained in the system. (administrator of classified data directory)

Rule 12. Confirm security - unless they contain secured data type security, do not consider data for secure. Once the type system treats data for secure. (manager lifecycle data management of classified data administrator events)

Rule 13. Confirm data storage - after confirmation of proper data security, the data is stored and the end user receives information about the stored data. (manager data life cycle, end-user storage medium, event manager)

B. *The life cycle of data storage*

The life cycle of data we want to store in the cloud takes place in several stages. Detailed specifications for individual stages and their relations shows diagram activity. The diagram consists of the communication between the end user, data, input data, and system directories. This data is checked through a database in which there are login client. After a successful login, the client provided input data – he works with and subsequently imposed.

The input data is provided from multiple sources (storage medium, external information system, etc.), and therefore it is necessary to check the availability of comprehensive data for the user. After checking the user it is able to work with data, which are classified into the security directory.

C. *Determined safety aspects*

If desired, increase data safety, it is necessary in the proposed model identify safety issues that affect the entire model..

The rules for user login

Rule 1. Insert login using the form.

Rule 2. Data can be verified through the database; the database is located on a server.

Rule 3. After successful verification, access is granted to the system and input data.

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-31

Rule 4. The input data is verified at intervals.

Rule 5. When you are finished with the end-user enters data requirements data storage.

The rules for encryption and data security

Rule 1. Data are categorized sensitivity (public, sensitive, secret); each category has a different certainty.

Rule 2. The level of security should at least be entitled; minimum entitlement. They are eligible for the end user for his work with the data.

Rule 3. Where the minimum privileges insufficient, it is necessary to establish new authorities; new permissions are assigned to the data set.

Rule 4. The system requires encryption after establishing authorization.

Rules for risks

Rule 1. Risks are designed to encrypt data; risks are procedures that cause data theft; database stores the risks that have been identified so far; if it is determined by a new risk is entered into the database; if the risk is already in the database, the changed, that related to data processing.

Rule 2. The security policy is based on the risks identified; security policy is a process to deal with the risk, which is recorded in the database.

Rule 3. The security policy demarcations of data protection; limit data protection determines appropriate and inappropriate practices for data; border data protection.

The rules for data integrity

Rule 1. The data are identified by assigning a specific value type in case of external storage media.

Rule 2. To ensure the data is assigned to data hash value.

Rule 3. To keep data integrity assurance do I determine the type of binding to the data; type of security is the degree, method and algorithm for data security. This value affects the limit of data protection, security policy, risk and minimal authorization.

Rule 4. The data is saved after completion of the previous rules.

Rule 5. If the end-user requests continuation of the deposit data, it is necessary to provide input.

D. Verification of the proposed methodology

The proposed model increased security of data stored in the cloud and established guidance. It has been verified in the environment medium businesses and universities. Verified by: a rough draft of architecture, infrastructure design, and implementation and testing technologies. These activities include the verification established safety rules.

Architecture

Architecture is basis for the methodology and implementation of cloud computing. To achieve a more global view of the architecture is not allowed to access the detailed architecture of the block, and therefore, they are determined in terms of a generally of the available options.

Based on the above theoretical basis article set out the following basic blocks of architecture: data, classification of data, data redundancy, key management, authorization levels, encryption system, TLS, HTTPS and latency setting.

Data

The architecture of the first block is further characterized by data identification, i.e. their origin, type, classification and the like. It's due to the fact that by the end-user is not appropriate for such information he granted or, as the end user only task is to insert data without knowing the detailed specification.

The proposed architecture supports three methods of data storage. In the enterprise environment it is a data entry mentioned risks. Inserting an external media is considered safe unless checking pins. Connection with external information systems it poses a risk for communication between systems that is secure, but may result in the interception.

In the university environment, the risk of end-user is consistent with the company environment. Within paste data from an external media control is possible only pins if the end user is using a right through university network.

Data classification

Submitted data should be classified. In the corporate environment are used 4 grading scale data. Public data they rebuilt the lowest level, which is not ensured in view of the proposed methodologies, since it is available in the global network Internet. These data strongly advise a general description of the company. Data for internal use are first secured degree. The originator data is either management that sends out information within the enterprise, or external information system that is secure. Third grade designation data is confidential and therefore data of a particular end user. Fourth, while the highest degree of safety data is confidential.

In the university environment is changing classification levels due to the type of data used and environment. The lowest level of public data remains unchanged. This is general information about the university, which are freely available. The originator data are academics, management of the university, students, external staff, administrators and the like. The third level includes data created and intended for the management of the university. For the development of these steps indicate that the original third classification level within the company at the university untapped, since data second grade designation in the university are available such as the Administrator, thus maintaining the confidentiality of individual data within university information system is irrelevant.

Data redundancy

In terms of data security and to maintain data integrity, it is necessary to store data redundantly. Therefore, in this architecture it works exclusively with redundant data. More detailed data redundancy in the design of infrastructure. In terms of corporate and university environments, it is important to observe redundancy data. The difference of the solution is to employ a hardware and software. Another the potential difference is the use of cloud services providers, and this option is more usable for the test medium enterprise

Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-31

than for the university due to technical availability and the number of end users.

Key management

Key management is closely related to authorization levels. Every end-user has a dedicated key on the basis of which work in the information system with data. The basis for communication is to establish session keys and universal key. The session key is used to manage communication within a given session.

Master key is used to verify the identity of the other parties, while assignment session key. For minimal security, it is necessary to ensure universal time keys with a timestamp (defined by time to expiration). Where the session acting as a third party, for example, center The distribution of keys is necessary compliance with confidence.

For each key is valid hierarchy of cities with keys, being preferred locale. As part of the key management is required to define each key authorized use. Using keys in communication between end users is necessary use SSH (Secure Shell). The basic features include SSH public keys is for future use. In terms of data security protocol SSH provides transparent transmitting data with a view to maintaining the integrity of data. The proposed model SSH is used in order to ensure access to the remote terminal computer.

Authorization levels

Readability level influence to legitimize the processing of data in the system.

In the corporate environment are specified following authorization levels: client of company has the lowest privileges within enterprise data, end-user is company employees, management of the company, IT department.

In the university setting authorization levels are defined on the basis described Tuncay´s model: potential candidates, university students, academics staff, management and IT department.

Algorithm to display the stored data based on the authorization level

```
publicList<string>GetFiles()
publicPath=Settings.Default.PublicPath;
confidentialPath=Settings.Default.Confide
ntialPath;
internalPath=Settings.Default.InternalPat
hList<string>listOfFiles=newList<string>()
;
if(Directory.Exists(publicPath))
strring[]fileEntries=Directory.GetFiles(pu
blicPath);
foreach(stringfileNameinfileEntries)
listOfFiles.Add(Path.GetFileName(fileName));
if(Directory.Exists(internalPath))
string[]fileEntries=Directory.GetFiles(int
ernalPath);
foreach(stringfileNameinfileEntries)
listOfFiles.Add(Path.GetFileName(fileName));
if(Directory.Exists(confidentialPath))
string[]fileEntries=Directory.GetFiles(co
nfidentialPath);
foreach(stringfileNameinfileEntries)
listOfFiles.Add(Path.GetFileName(fileName));
returnlistOfFiles;
```

Encryption system

The basis of this algorithm selection was a high deliverability maintaining the integrity data and support for file integrity. Extended hash function SHA It is used with SSH and SSL. Based on these premises and testing I recommend SHA for use in corporate and university environments.

TLS

TLS is a layer for secure communication, and thus cryptographic protocol. Despite the fact that the theoretical bases of the above recommendation the SSL in this work is used TLS. TLS is successor of SSL. SSL encryption system fully supports SHA, connection authentication code (MAC code) for file storage and encryption. [14]

Unless the company wants to use the SSL protocol and it is necessary to use other protocols such as IMAP. For security authentication these protocols were also used beast attack (assault BEST), which completely broke page running under SSL version 3 and TLS version of the first Therefore, when using TLS to use the current version as well as in corporate, as well as in the university. [15]

HTTPS

HTTPS is suitable for increased safety in the information system in the enterprise and the university, as it is primarily intended for dynamic content that is not publicly available. Within the connection through this protocol is not you can create multiple virtual Web servers on a single IP address. His disadvantages are slowing system response.

Latency setting

Based on the theoretical basis it is appropriate to determine the length of the latency in communication. However, the results of the testing demonstrate the opposite, and therefore the determination results in latency system slowdowns and provide low security. As the proposed system should have a fairly good response, it introduced the unlimited latency and thus not limiting seating end user.[16]

E. Infrastructure

The proposal is a generalized infrastructure for business and university environment, while it has been verified within the university (Figure 1).

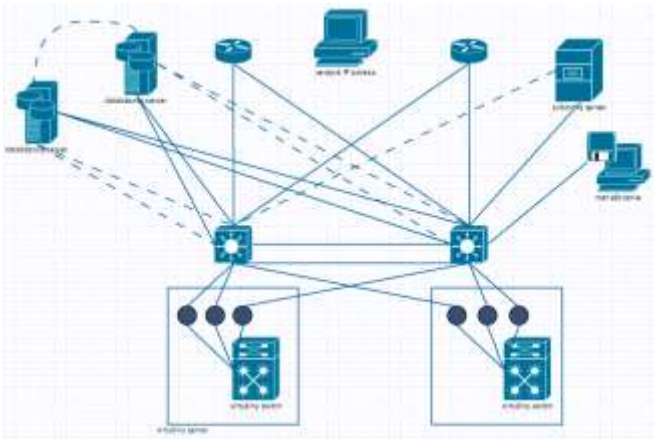

Figure 1. Infrastructure of network

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-31

IV. Summary

The primary factor for maintaining data security is established business rules. The form of these rules is usually because internal. It has not yet been established metrics and general framework methods to improve safety data stored in the cloud.

The second important factor is the employee of firm. For integration work of employees in carrying out their functions are recommended training in order to explain the importance of data security methods and security. Training should also respond to the business and risk policy to help employees understand risk identification and manner of execution.

Next step is monitoring events and creating audits. Monitoring events reports risky procedures and identifies potential threats as part of the client and server-side. Regular auditing is accomplished for the purpose of identifying possible ways of their solution, and alienation.

The proposed framework methodology agglutinates identified restrictions against rules end user encryption and data security and integrity risks identified data based on the theoretical results referred to in work and transferred testing.

The methodology is set so that it can be implemented small, medium-sized enterprises and universities. The deployment of this methodology provides stable system data security solutions in implementing the environment.

The verification methodology were tested set-up of the defining block architecture client-server, network infrastructure design data of the central storage, compilation and editing data storage hardware, implemented KVM virtualization technology solutions and data integrity using the file ZFS.

Transferred repair of hardware in the form of the introduction of the RAM disk has shown that it. It is the optimal solution for data security, but its safety can be increased duplication of the network to multiple servers or slowing sync with SSD discus. By testing a file system ZFS is found that at a 95 percent reaching and higher occupancy file system becomes a performance file system almost unusable.

References

[1] Sosinsky, B. Cloud Computing Bible. New York: John Wiley and Sons, 2011.

[2] Winkler, V. Securing the Cloud. New York: Syngress, 2011.

[3] Hurwitz, J. Hybrid cloud for dummies. New York: John Wiley Sons, 2013.

[4] Hayes, B. Cloud computing. ACM, 2008.

[5] Sclater, N. Cloudworks, eLearning in the Cloud. [online]. [cit. 2013-06-09] Available: http://cloudworks.ac.uk/cloud/view/2430.

[6] Yang, K. Security for Cloud Storage Systems. Londýn: Springer, 2014.

[7] Microsoft. SME role for cloud computing. [online]. [cit. 2013-08-09] Available: http://www.microsoft.com/uk/smallbusiness/sbnews/growing-asmall-business/SME-role-forcloudcomputing-19227631.mspx.

[8] Tuncay, E. Effective use of cloud computing in educational institutions. Procedia: Social and Behavioral Science, 2010.

[9] Klein, C., Kaefer, G. From smart homes to smart cities: Opportunities and challenges from an industrial perspective. Lecture Notes in Computer Science, 2008.

[10] Lijun, M., Chan, W. K., Tse, T. H. A tale of clouds: Paradigm comparisons and some thoughts on research issues. IEEE, 2008.

[11] Praveena, K., Betsy, T. Application of Cloud Computing in Academia. London: HM, 2000.

[12] Delic, K. A., Riley, J. A. Enterprise Knowledge Clouds: Next Generation KMSystems? Kankun: ICI, 2009.

[13] Erikson, J. S., Spence, S., Rhodes, M., Banks, D., Rutherford, J., Simpson,E Content-Centered Collaboration Spaces in the Cloud. IEEE, 2009.

[14] Lim, I., Coolidge, E., Hourani, P. Securing Cloud and Mobility: A Practitioner´s Guide. New York: CRC Press, 2013.

[15] Ming, L., Shucheng, Y., Kui, R., Wenjing, L., Thomas, H. Toward privacyassured and searchable cloud data storage services. IEEE Network, 2013.

[16] Thuraisingham, B. Developing and Securing the Cloud. New York: Auerbach Publications, 2013.

About Author (s):

ZUZANA PRIŠČÁKOVÁ

She graduated at Faculty of Natural Sciences UKF Nitra in 2012. From graduating she began studying doctoral studies at Faculty of Business and Economics MENDELU Brno in 2012. In 2014 she graduated her doctoral study in applied informatics.
In 2010-2011 she worked as an assistant of IT project manager. Since 2013 she has worked as an academic staff (assistant) on the Department of informatics MENDELU in Brno.
In 2014 she taken part in internships at Faculty of Cybernetics Taras Shevchenko National University of Kyiv.
Her research is focus on data integrity, data security in cloud computing and IT project management.
In 2013-2014 she was the solver of project Deployment of open-source virtualization technology at MENDELU.

IVANA RÁBOVÁ

She graduated at Electronic faculty VUT Brno in 1981. In 1990-1996 she worked as a leader of the information systems department in a large company in Brno. Since 1997 she has worked as a university teacher on the Department of informatics PEF MZLU in Brno. In 2002 she graduated her doctor study and she obtained Ph.D. In 2006 she was habilitated in Management informatics subject the name of her thesis is Enterprise Architecture; Analyse, Modeling and Value in Business Management.
She was the solver and co-solver of several projects of innovation education within the scope.