SECURITY SOLUTION FOR CLOUD COMPUTING

Lukasz APIECIONEK

Kazimierz Wielki University, Faculty of Mathematics, Physic and Technical Sciences, Poland

e-mail: lapiecionek@ukw.edu.pl

Michał ROMANTOWSKI

Warsaw School of Economics, Poland

e-mail: mromantowski@wp.pl

Abstract

A concept of Cloud Computing is currently widely applied. Users that benefit from data storage capability and applications on demand access may use resources easily, using various devices. However, such solutions as CC require taking into consideration issues related to security. A problem of assuring safety of data, that is stored in the cloud, in different sites is a significant challenge. It seems necessary to elaborate standards and mechanisms of assuring stored data security and integrity. This article presents a practicable appliance of mechanisms created by NATO that after a suitable adjusting may be used for securing data stored in a cloud. A general concept of such mechanism is presented. In addition, a ready to apply solutions are included, which may considerably shorten putting a CC into practice.

Keywords**:** *security, cloud computing, IP network*

1 INTRODUCTION

Cloud Computing (CC) is currently widely applied. Cloud is a fresh approach towards utilizing resources, rather than a new technology. This approach makes possible a significant operating cost reduction. Users, that benefit from data storage capability and applications on demand access, may use resources easily, using various devices and take advantage of this opportunity for quite a long time [1] [2] . However, such solutions as CC require taking into consideration issues related to security. A problem of assuring safety of data that is stored in the cloud, in different sites is a significant challenge. A present lack of security standards and difficulty with its determination and appliance, along with no confidence limits broader implementation of CC [3] [4] [5] . It seems necessary to elaborate standards and mechanisms of assuring stored data security and integrity. This article presents a practicable appliance

of mechanisms created by NATO, that after a suitable adjusting, may be used for securing data stored in a cloud. The chapter 2 consists of:

- widely described in literature security issues of storing data in cloud,
- concepts of access gateways, that have been elaborated by NATO,
- possible appliances of gateways in Cloud Computing,
- particular gateway implementations descriptions, including their test results.

Last part of the article contains a summary of presented matters followed with conclusions.

2 CLOUD COMPUTING SOLUTION

2.1 Problem description

A Cloud is a perfect solution for business. It provides cost reduction, while with little infrastructure investment one can quickly obtain an access to multiple services. On the other hand a trust and its complicity is an issue. Security matters have to be considered globally, at the point when a computer system is built, certainly not after having the system created. At the initial level of designing a system, ways of providing security and trust should be considered. It is assumed, that there is no point developing a one, common solution dedicated for every possible scenario [6]. An emphasis on security issues evolves continuously. At the beginning they were related mostly to hardware protections, next on some end point restrictions, while for now it is often considered at an application level.

A providing data security issue appears usually, when a cloud management is outsourced to a cloud provider. There is a little warranty and certainty of proper responsibilities execution and providing data security. It is common, that a provider transmits data between different data centers. However, in some cases particular data should not be transferred to a particular data storage point, because of security restrictions, and transferring may result in unattended data access or manipulation. Therefore data should be properly marked, to enable its recognition [3] [7] [8] [9] . In CC users are determined to be responsible for data security, by marking data in a proper way. This requires creating systems capable of marking data [10] . It should be possible to move virtual machines between different physical locations and applications should contain no restrictions concerning working location. However, creating such applications, regarding law regulations and business requirements is complex [11]. A capability of moving machines indicates, that a system architecture changes continuously. This results in another issue, related to monitoring a cloud based system, which is highly complicated and widely described in literature because of a volatile infrastructure and no monitoring workstation stability confidence [12] [13] [14] [15] . In literature certain ways of transferring virtual machines between different locations can be found [16] . A transfer and proper data storage monitoring is entrusted to so called TPA (Third Party Auditor) [17] [18] [19] . Nevertheless, simultaneously

the literature [20] [21] analyzes how virtual technologies improve the system security, and it is indicated that the virtualization has incalculable impact on the security enhancement on at least three aspects:

- it can easily isolate and shield unstable applications or those with security risks,
- support powerful sound crime analysis and highly effective disaster recovery solutions,
- virtualization also provides intrusion detection tools of lower costs.

However CC users need to be informed about every mentioned security related aspect [22] [23] , it is required to change a traditional security means to a new approach based on a new thinking [24] .

In order to increase the security certain mechanisms need to be determined, that provide:

- labeling (marking) data,
- controlling a cloud with TPA.

Such solution has its disadvantage – a TPA requires a cloud access, is able to control it at a particular time, but is unable to provide continuous monitoring. What is more, such solution is costly, as it requires an external auditor.

2.2 Information Exchange Gateway Concept

NATO is in the act of adaptation a NNEC concept (NATO Network Enabled Capability) and discarding the idea of building systems in favor of creating services. NNEC is one of the fastest developing and spreading concepts designed for network-centric purposes and is intended to speed up and simplify decision making on the battlefield. To achieve the goals of this concept, a main challenge to be faced was an automated networks connection. It requires an implementation of Information Exchange Gateways (IEG), that fills the existing air gaps, one-way data diodes or in some rare cases the existing non-administered two-way connections.

At the strategic level, a task of an IEG is to support a process of political consultation and allow a national planning and more effective orientation of operations and at an operational level it is to support daily operational planning and management. At the tactical level an IEG enables an improved presentation of information for commanders and better understanding of their intentions, a possibility of sharing information with coalition members, a dispersed cooperation and a network integration of collectors, decision makers and effectors [25] .

According to the NATO concept, in an IEG three basic functional elements can be distinguished [26] :

- NPS (Node Protection Service) – its task is to protect physically IEG infrastructure. It is usually executed by a specialized firewall with implemented mechanisms of protection against attacks;
- IPS (Information Protection Service) – its task is to protect and control the flow of information. IEG characteristic does not require this service to be in

physical proximity of IEG. It is only required that the whole traffic into and out of IEG is managed by this service by means of NPS;

- IES (Information Exchange Service) – it has to provide the flow of information between the protected node and an outside, authorized (using IPS) organization. Only the information that IES can transfer should be transported by IEG. The example of this kind of information are e-mail service protocols, http, directory services, Web service and many more.

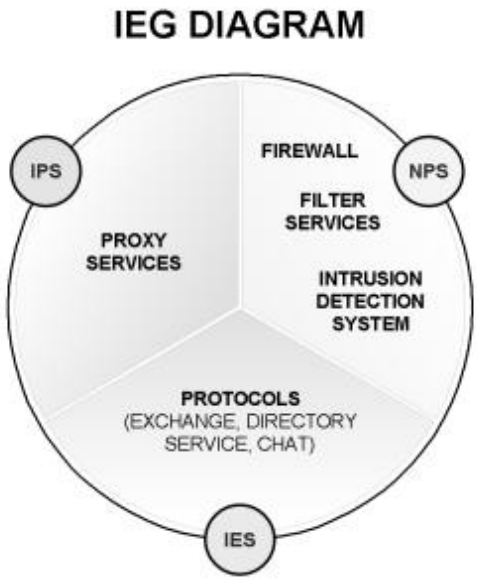

Figure 1 IEG Diagram [26]

An IEG is installed to protect a network from possible attacks, viruses and intruders. At the same time it checks the flow out to make sure that the information can be disclosed.

To ensure a proper control of transferred data, the data is self needs to be marked. In order to obtain that, a developed standard may be used – an XML Security Labeling (*farther referred to as security labels*), which is a NATO standard used to define a security policy. Generally speaking a security label is a document compliant with XML standard describing a security classification and an importance level of digital data. Such a label can be enclosed to any digital source. It often contains metadata concerning document digital in a form compliant with XML-Sig standard. According to a way of placing a label three types of labels can be distinguished: packed, packing and split.

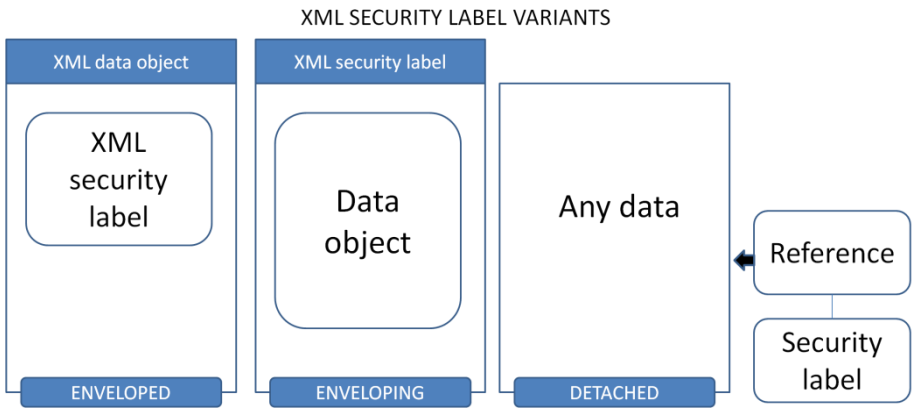

Figure 2 Kinds of security label [26]

In a peculiar case, when a security label is a part of an XML document, a security classification may concern not only the whole document but also its particular fragments denominated by means of XPath expressions. It provides a user additional possibilities of creating security policy, by granting a different secrecy classification to pieces of information within one document. Sending information about location of a unit may serve as an example. Its coordinates are available to anyone (NATO UNCLASSIFIED clause), whereas information about its name is classified, which can be seen in a fragment of an XML document.

```
<target>
  <coordinates>
     <x>12345</x>
     <y>67890</y>
  </coordinates>
   <SecurityLabel
       xmlns:slab="http://nc3a.nato.int/2004/06/xmlslab#">
     <LabeledObjectGroup Id="myLabeledObject">
       <ConfidentialityLabel>
         <SecurityPolicyIdentifier>
           NATO
         </SecurityPolicyIdentifier>
         <SecurityClassification>
           UNCLASSIFIED
         </SecurityClassification>
         <SecurityCategory type="Permissive">
           RELEASABLE FOR INTERNET TRANSMISSION
         </SecurityCategory>
       </ConfidentialityLabel>
       <dsig:Reference URI="">
```

Informations about unit coordinates

Security Policy Identifier

Security Classification

Security Category

Figure 3 Example part of a XML document [26]

2.3 Information Exchange Gateway As A Solution For Cloud Computing

Considering an IEG as an appliance for CC requires answering questions related to providing security of a transferred data. This determines whether an IEG possibly improves a cloud architecture with a positive influence on its security aspect. Firstly, in order to apply an IEG it is required to:

- mark data, that are stored in a cloud according to a specific, determined standard (possibly one determined by NATO),
- mark entire virtual machines, that are exploited by users and the labeling standard has to be developed,
- control an outgoing traffic,
- control a virtual machines flow between data centers,
- control a data access.

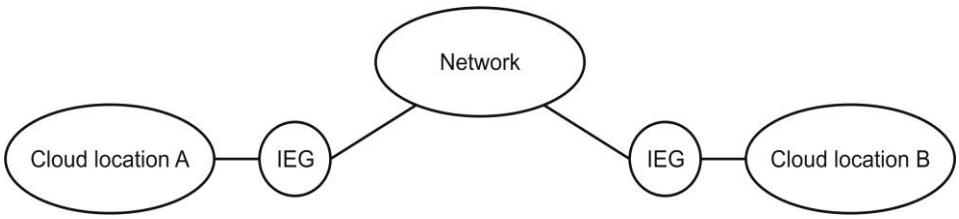

Figure 4 Cloud computing connection through IEG

Introducing a transferred data control with such solution as an IEG may ensure a continuous infrastructure surveillance, with no TPA. A TPA, instead performing all the time supervision may be exploited to audit the system, whether an IEG infrastructure is properly connected and operating.

Having above stated conditions fulfilled, a cloud computing may be used in wider scenarios. An IEG controls user data and services access and virtual machines transfer between locations. In case either data, service, or virtual machines is labeled in a way, that does not allow transferring to other location, an IEG blocks transmission.

2.4 Practical implementation

It should be pointed out, that a suggested approach is an existing, working and ready to apply solution. Two widely evaluated during international CWIX [28] exercise IEG class solutions exist:

- IEG JASMINE,
- Safe Exchange Information Gateway.

IEG JASMINE is a solution developed by TELDAT company. It was adjusted for military appliances. IEG JASMINE has a modular structure – each of its components

fulfills particular goals, that have been set in the specification. The basic module is a Firewall Box which is responsible for a security control at the lowest network level and serves directly as NPS (Node Protection Service) in an IEG model. A Firewall Box functions include an intrusion detection and prevention system IDS/IPS. A basic task of the module is to perform the analysis of network flow regarding the content and directing it to destination modules.

An IEG CS (Core Service) JASMINE module is responsible for controlling the flow of information for the basic services: an e-mail, directory services and messaging. An IEG FS (Functional Service) JASMINE module is responsible for filtering all the additional services supported by C3IS JASMINE system [25] .

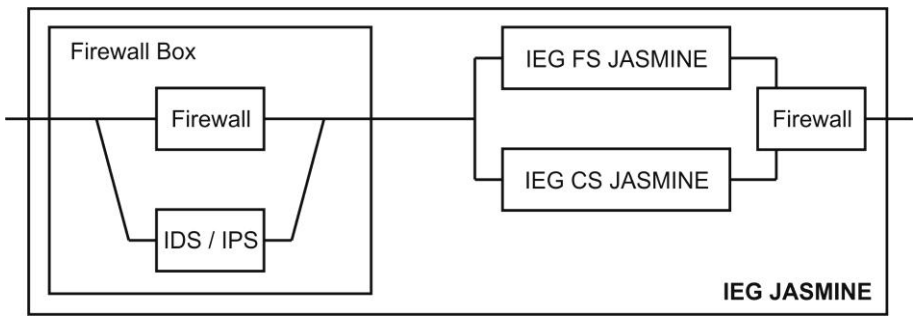

Figure 5 Structure of IEG JASMINE [25]

A Secure cross-domain Information Exchange Gateway is a concept of boundary protection device that enables information sharing between cooperating domains with different security levels. It is based on the NATO idea of secure information sharing in cross-domain relations based on IEGs and consists of several cooperating elements, i.e.:

- 2 x NPS – one for each security side,
- 2 x set of protocol proxies – one set for each security side,
- XML guard.

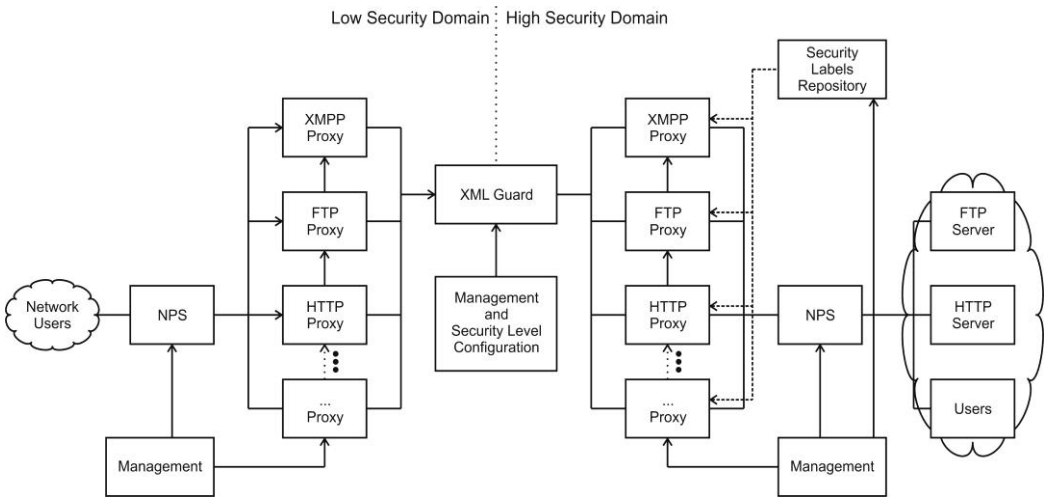

Figure 6 IEG architecture [29]

Protocol Proxies are dedicated for analysis of particular protocol (such as FTP, HTTP etc.), that converts data stream into HTTP/SOAP message containing security label. XML Guard is a central SIEG component responsible for a security policy execution during data exchange. It is the only element that physically connects both domains. This is where a security label is evaluated against its integrity and validity, and where the permission to pass the data to the other domain based on the predefined security policy rules is obtained [29] .

A CWIX exercise goal is to evaluate different national solutions against its interoperability in multinational environment. As it has been stated before, both above described systems have been tested during CWIX in 2012. An IEG JASMINE has been evaluated against following protocols:

- XMPP,
- SMTP/POP3,
- HTTP,
- and military data Exchange protocols MIP DEM Baseline 3, NFFI (IP1, IP2, SIP3).

A SIEG evaluation was performed using:

- XMPP,
- SMTP/POP3,
- HTTP.

An evaluation included few factors: a protocol compliance, a proper transmission control, a security policy execution and an end user work experience. Both systems fulfilled mentioned criteria in each protocol test suite. Though significant transfer

delays were expected, an evaluation revealed, that data transfer delays are unnoticeable for a end user and have no impact on an electronic mail transfer, a Web browsing and an XMPP based text communication.

It should be pointed out, that a dedicated appliance for a Cloud Computing requires performing further tests, considering performance for significant user number, and such evaluation has to be done.

3 SUMMARY

This article presented military standards, that are applicable to Cloud Computing architecture and, as a result, increase its security. However, such appliance requires preparing minor extensions to described systems, including implementing a new IEG JASMINE module and developing a protocol proxy for SIEG solution. Therefore, after this slight expense, a CC benefits from extended protection capabilities. This includes an enhanced control over transmitted data and moved virtual machines and a TPA role change. As it has been stated, in such case a TPA becomes an additional auditor, instead of single party, that guarantees a appropriate security. This paper proves, that existing security solution is possible to be applied and will bring a new quality to CC.

REFERENCES

[1] HORRIGAN, J. B.: Cloud Computing Gains in Currency, 2008, at http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency

[2] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, at http://www.cloudsecurityalliance.org/topthreats, 2010

[3] MACE, J., VAN MOORSEL, A., WATSON, P.: The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments, in The First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV 2011), China 2011

[4] SUBASHINI, S., KAVITHA, V.: A survey on security issues in service delivery models of cloud computing. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.07.006\

[5] SHARMA, P. D.: A classification of distinct vulnerabilities in cloud computing, World Journal of Science and Technology, Vol. 2, 2012

[6] PEARSON, S.: Toward Accountability in the Cloud, View from the Cloud, IEEE Internet Computing, IEEE Computer Society, July/August issue, vol. 15, no. 4, pp. 64-69, 2011

[7] HAY, B. , NANCE, K., BISHOP, M.: Storm Clouds Rising: Security Challenges for IaaS Cloud Computing, Proceedings of the 44th Hawaii International Conference on System Sciences - 2011, Print ISBN: 978-1-4244-9618-1

[8] CHEN, D., ZHAO, H.: Data security and privacy protection issues in cloud computing, in Proceedings of the Inter-national Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 647–651

[9] TRIPATH, A., MISHRA, A.: Cloud Computing Security Considerations, IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE
[10] ALMORSY, M., GRUNDY, J., IBRAHIM, A. S.: Collaboration-based cloud computing security management framework, IEEE 4th International Conference on Cloud Computing (CLOUD 2011), Washington DC, United States, 04-09 July 2011, 364-371. Piscataway, NJ: IEEE
[11] ROCHWERGER, B., BREITGAND D., EPSTEIN, A., HADAS, D., LOY, I. NAGIN, K.. TORDSSON J., RAGUSA C., VILLARI, M., CLAYMAN, S. LEVY, E., MARASCHINI, A., MASSONET, P., MUN, G., TOFETTI, H.: Reservoir—When One Cloud Is Not Enough, IEEE Computer, March 2011, pp. 44-51
[12] IYENGAR, M. S., ARUN, K., ROUVELLOU, I. M, LING, L., KISUNG, L.: Reliable State Monitoring in Cloud Datacenters, Conference Publications, Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on Page(s): 951 - 958, ISSN : 2159-6182, Print ISBN: 978-1-4673-2892-0
[13] SPRING, J.: Monitoring Cloud Computing by Layer, Part 1, THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/11/$26.00 © 2011 IEEE, MARCH/APRIL 2011, pages 66-68
[14] SPRING, J.: Monitoring Cloud Computing by Layer, Part 2, THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/11/$26.00 © 2011 IEEE, MAY/JUNE 2011, pages 52-55
[15] JANSEN, W., GRANCE, T.: Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, December 2011
[16] WATSON, P., A Multi-Level Security Model for Partitioning Workflows over Federated Clouds, Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1271
[17] WANG, Q., WANG, C., REN, K., LOU, W, LI, J.: Enabling public auditability and data dynamics for storage security in cloud computing, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011
[18] WANG, C., CHOW, S. S.-M. WANG, Q. REN, K., LOU, W.: Privacy-preserving public auditing for secure cloud storage, Cryptology ePrint Archive, Report 2009/579, 2009. http://eprint.iacr.org/
[19] RAMANE, M. ELANGOVAN, B.: A metadata verification scheme for data auditing in cloud environment, International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.4, August 2012, pp. 53-62
[20] WU, J. SHEN, Q., WANG, T., ZHU, J., ZHANG, J.: Recent Advances in Cloud Security, Journal of Computers, Vol. 6, No. 10, October 2011
[21] WEINHARDT, C., ANANDASIVAM, A., BLAU B., STOSSER, J.: Business Models in the Service World, IT Professional, vol. 11, pp. 28-33, 2009
[22] BUYYA, R., YEO, C. S., VENUGOPAL, S.: Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. CoRR, (abs/0808.3558), 2008

[23] CARLIN, S., CURRAN, K.: Cloud Computing Security, International Journal of Ambient Computing and Intelligence, Vol. 3, No. 1, pp:38-46, April-June 2011, ISSN: 1941-6237, IGI Publishing

[24] KO, R. K. L., KIRCHBERG, M., LEE, B. S.: From system-centric to data-centric logging - Accountability, trust & security in cloud computing, Defense Science Research Conference and Expo (DSR), 3-5 Aug. 2011

[25] APIECIONEK, Ł., WOŹNIAK, M., ROMANTOWSKI, M., ZNANIECKI, W.: Information assurance in coalition mission environment, Military Communications And Information Systems Conference (MCC), Wrocław 27-29.09.2010

[26] Guidance document on the implementation of gateways for information exchange between NATO and external CIS communities, version 1.21 dated 16th February 2007 AC/322(SC/4)N(2007)0007, MULTI REF

[27] THUMMEL, A., OUDKERK, S.: Technical Note 1330 - XML-LABELLING GUARD HIGH LEVEL DESIGN EDITION 1,

[28] http://www.act.nato.int/news-stories/cwix-2012-creating-joint-warrior-interoperability

[29] APIECIONEK, Ł., ROMANTOWSKI, M., ŚLIWA, J., JASIUL, B., GONIACZ, R.: Safe Exchange of Information for Civil-Military Operations, Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011