Experimental Evaluations of the Impact of High availability on the Quality of Protection of Hybrid Clouds

Syed Naqvi, Michael Van de Borne, Arnaud Michot

Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)
29 Rue des Frères Wright, 6041 Charleroi, Belgium
{syed.naqvi, michael.vandeborne, arnaud.michot}@cetic.be

***Abstract*—A common perception of security services is an overhead on distributed system's performance that exponentially increases with scale and heterogeneity of the system's components. While this perception is not untrue, there is no precedence of experimenting the exact impact on its overall performance in terms of quality of protection. This paper presents a formal way of testing the impact of scalability and heterogeneity on the federated Cloud security services. The work presented in this paper aims to develop a mean of quantifying the impact on security functions under various operating conditions and parameters of federated Cloud deployments. The results of this experimental study will help businesses to identify the best security architecture that will fit their Cloud architectures and performance requirements.**

Keywords-Cloud computing; security architecture; performance parameters.

I. INTRODUCTION

Monitoring of security performance is an established requirement of highly available services and infrastructures [1]. Moreover, insight into the composition of security mechanisms is one of the research areas identified by the United States National Institute of Standards and Technology (NIST) in its report on directions in security metrics research [2]. However, as of today, most of the proposed approaches only deal with the monitoring of application level security measures such as monitoring of antivirus updates, installation of patches, IDS (intrusion detection system) buffer monitoring, etc. The range of available commercial products to perform security monitoring generally examine various high level parameters. For example, Cisco's MARS (Monitoring, Analysis and Response System) [3] is designed to monitor logs and to monitor threats; Hewlett Packard's IT Performance Suite [4] is designed to monitor security and risk management processes (such as number of systems under security control, risk indicators, etc.). However, none of these tools provide any information about the monitoring of the impact on security at the infrastructure level.

It is generally understood that security takes its toll on system performance; and providing consistent security to scalable distributed systems requires careful consideration of performance overheads [5]. However, no tangible efforts are made to quantify the performance degradation by relating the quality of protection with the system performance. The knowledge of the impact of security at infrastructure level is particularly important to cope with the emerging challenges of hybrid Clouds such as scalability, heterogeneity, criticality of their applications, etc. It is therefore important to determine an empirically validated function for security services: on different application loads; for a number of virtual machines; on different cloud technologies; with different types of hypervisors.

In this paper, we present our security monitoring experiment that aims to examine the implications of security on the back-end system of emerging realm of IT services - i.e. hybrid Cloud infrastructures. This experiment - ExSec: Experimenting Scalability of Continuous Security Monitoring - is one of the experiments of European Future Internet experimental facility and experimentally-driven research project BonFIRE [6]. Main objectives of the ExSec experiment is to study and quantify the impact on the quality of protection of Future Internet based applications that will be highly scalable in nature and use heterogeneous underlying technologies. These experimental evaluations will be useful to determine the *stretching limit* of Cloud security functions; and eventually, workout some remedial solutions especially to explore the possibility of making use of abundance of Cloud resources to compensate the performance degradation.

The test scenarios of the ExSec experiment are designed to reflect real-life situations where in a routine business context, organizations forming a virtual organization (VO) are most likely to run heterogeneous cloud managers; and hence the situation often arises where hypervisors of different types using different virtual execution environment managers are required to collaborate to form a VO. The bottom line of this study is to develop a mean of quantifying the impact on security functions under various operating conditions and parameters of Cloud deployments.

The rest of this paper is organized as: Section II outlines the context of our work. A set of security policy rules and impact factors are outlined in Section III. The experimental set up of our study is detailed in Section IV. Section V provides a pragmatic discussion of the scope and perspectives of our work. Finally, some conclusions are drawn in Section VI together with a brief account of our future directions.

 ISBN: 978-1-61208-209-7

II. CONTEXT AND MOTIVATIONS

A. Background of Experimental Study

We implemented a security framework for Grid computing environments in one of our previous European projects - GridTrust [7]. This work included a prototype implementation of the *Usage Control (UCON)* concept in the context of virtual organizations (VO). This work consisted of a vertical approach for Grid security from requirements level right down to application and middleware levels. The GridTrust framework provides policy-driven autonomic access control solutions that provide a continuous monitoring of the usage of resources (usage control) by users. This groundwork on the deployment of UCON model in the security framework of a highly distributed environment gave us an insight in the problematic of security monitoring; and the awareness of the impact of scale on security performance. Unlike access control, usage control perpetually monitors security parameters and is directly affected by the scale of the system being controlled. Therefore, its impact on the performance may become significant enough to be overlooked. However, to the best of our knowledge, there is no formal way of quantifying this relationship or to extrapolate it for complex scenarios.

We explored the monitoring of Cloud security services in the European Cloud computing flagship project RESERVOIR [8] with particular focus on the audit logging for data location compliance issues. The underlying Cloud technology used in the RESERVOIR project was OpenNebula [9] that was uniformly deployed across various sites of the RESERVOIR Cloud. We are therefore using a FIRE (Future Internet Research Experimentation) facility - more precisely the BonFIRE project - now to have access to a large-scale heterogeneous Cloud environment that provides opportunity to perform tests on real infrastructures of scale. Moreover, our study is facilitated by a range of technical solutions provided by the BonFIRE infrastructure such as monitoring tool (ZABBIX [10]), client library for RESTful APIs (RESTfully [11]), JSON [12] interface for data-interchange, etc.

B. Related Work

Most of the ongoing Cloud computing endeavors are still pointed to the challenges of their large scale deployments. Security is undoubtedly the cornerstone of these deployments; however, the progress in this area is still in its earlier stage. Therefore, not too many initiatives are taken in this direction so far. Some of these approaches are evaluated in this section.

CloudSec [13] provides active, transparent and real-time security monitoring for multiple concurrent VMs hosted on a Cloud platform in an IaaS setting. CloudSec employs VMI (virtual machine introspection) [14] for monitoring VMs at the hypervisor level. CloudSec aims to protect kernel data structures. However, it does not address the impact of these multiple concurrent VMs on Cloud platform security.

Another important security area where monitoring technology has an important role to play is digital investigations. Security monitoring can facilitate conception of forensic friendly IT infrastructures such as electronic communications [15]. Reliability of monitoring data is of prime importance in this domain as the validity of data as an *acceptable proof* in court of law is crucial in digital investigations. This aspect of security monitoring is useful to keep track of security information. However, it does not offer any solution to the problem of estimating the accuracy of security monitoring for a particular scale and its dependence on specific underlying technology.

Our work presented in this paper is a pioneer initiative in the direction of quantitative analysis of the impact of scalability and heterogeneity on security functions. This work will enable businesses to deploy some Cloud solutions with optimal security architecture that will fit to their Cloud architectures and performance requirements.

III. SECURITY POLICY FOR THE EVALUATIONS

This section outlines the security policy for the ExSec experiment's evaluations. The overall objective of this rigorous security policy is to ascertain a real life situation that will use the federated cloud infrastructure for its routine operations. The nature and scope of such paradigm will require simultaneous fulfillment of several policy rules. This situation will strain the overall security policy enforcement mechanism in general; and its policy decision point (PDP) in particular.

A. Scenario description

The security policy scenario depicts a Future Internet based social application where access to digital contents (such as music files) requires a number of conditions to be satisfied such as:

1. The foremost condition is to ensure that the subject has paid for the contents he/she intends to access.
2. The type of contents (e.g. latest songs or the songs released a couple of years before the access request)
3. The type of access (e.g. premium for priority download, or ordinary for slower download speed)
4. The access limit (e.g. unlimited access or some limits are applied such as maximum number of songs that can be downloaded in a given time; specific download time – night only, weekend only, etc.
5. The geographical location of the user to protect the rights of the digital distributions.

Moreover, a number of events may raise suspicions leading to some corrective measures such as:

1. If a user with individual subscription simultaneously attempts to access the contents from different locations.
2. If a user makes more than a specific number of futile attempts to access the contents.

Figure 1 depicts a non-exhaustive list of major decision parameters for the Policy Decision Point (PDP) for the abovementioned Future Internet based digital contents application. The impact of the range of these parameters on the performance of PDP is exacerbated when a big number of (scalable) requests are concurrently made to the

 ISBN: 978-1-61208-209-7

application gateway. We aim to quantify this impact and establish relationship between the load on the PDP and its impact on the performance. System calls are intercepted to have a lower level control over the incoming requests. Major security challenges of this scenario are to ensure firm access control despite higher scale of requests; to enforce usage control policies; and to cope with the heterogeneity of the underlying technologies.

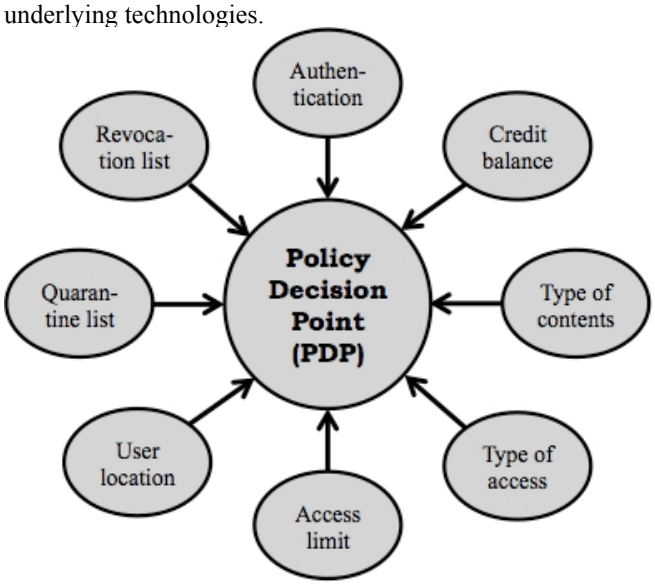

Figure 1. Overview of the security policy scenario

B. Policy rules

This section summaries some example security policy rules and the impact parameters to be studied in the course of ExSec experiment.

1) Access control policy rules

- **AC1:** Access to digital contents files is restricted to users in good standing
- **AC2:** Have enough credit for requested digital contents
- **AC3:** Maximum number of digital contents files is not reached
- **AC4:** Access digital contents from the eligible location

2) Usage control policy rules

- **UC1:** Maximum number of downloads granted
- **UC2:** Maximum number of downloads in a specific time (e.g. per hour)
- **UC3:** Maximum number of downloads of specific type of files (e.g. classical music)

3) Monitoring policy testing scenarios

- Security verification for an end-user web application running on the same underlying VM Host technology - for example KVM.
- Security verification for an end-user web application running on the different underlying VM Host technologies - for example KVM and Xen.
- Security verification for an end-user web application running on the same underlying Cloud engine - for example a sub-experiment on OpenNebula or a proprietary technology such as the one offered by the HP for BonFIRE.
- Security verification for an end-user web application running on the heterogeneous Cloud engines - for example, a cloud management environment composed of OpenNebula and HP technology.
- Security verification for a completely heterogeneous environment with diverse VM Hosts and Cloud engines.

4) Impact parameters

- Gradually increase number of clients (download requests) to get access to digital contents file (cf. network throughput, CPU utilization, RAM, etc.)
- Add timeslot constraint for the download requests (maximum number of permissible downloads per hour)
- Add file type constraint for the download requests (type of digital contents that can be downloaded – e.g. files of type A, B, and C)
- Add location constraint for the download requests (such as number of download requests per server)
- Placement of PEP/PDP
- Within a VM
- One at each BonFIRE site
- One for the entire infrastructure

IV. EXPERIMENTAL SETUP OF OUR STUDY

A security policy enforcement architecture using XACML [16] is deployed as a first step of this study so as to secure access to the BonFIRE resources. This security policy enforcement architecture is shown in Figure 2. Access to the BonFIRE infrastructure is based on the authentication mechanism where we have installed a filter to intercept all HTTP requests sent to the ExSec experiment's WebApp. This filter constructs an XACML request with the client information (e.g. the requesting IP address). The Policy Enforcement Point (PEP) invokes the *AccessControl* service followed by the evaluation of access request by the Policy Decision Point (PDP) that returns TRUE if the access is permitted, or FALSE otherwise. The interactions of PEP and PDP together with their port numbers are provided in Figure

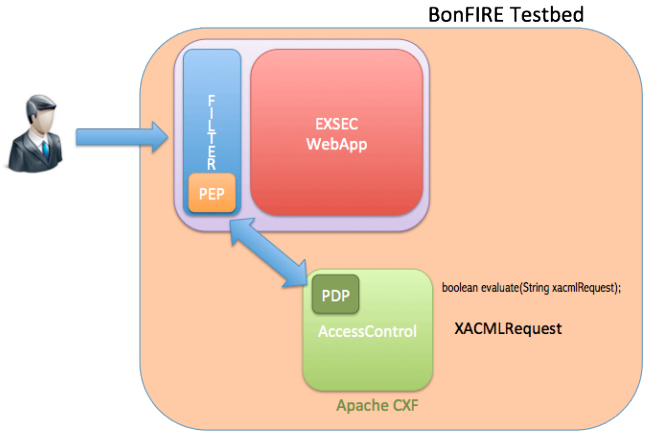

Figure 2. ExSec credentials management system

3. Additional filters will be used for monitoring of security parameters by using UCON model.

We now present fine-grained architectural information of our proposed architectural set-up. We first describe different schemes of placing security policy enforcement points (PEP) in the BonFIRE computer resources followed by the number of testing scenarios for the study.

A. *Case-1: When PEP module is integrated inside server node*

Jikes Java Virtual Machine (JVM) launches a RESTlet HTTP server. Every system call from this REST server to gain physical access to a file (e.g. to open a file) is intercepted by the Jikes JVM, which queries the PEP module. The latter applies the Usage Control security policy (i.e. one download at a time), and returns this answer to Jikes, which grants or denies the physical access request for a file. In this case, there is a PEP module shipped with each compute node. This scheme is presented in the Figure 3.

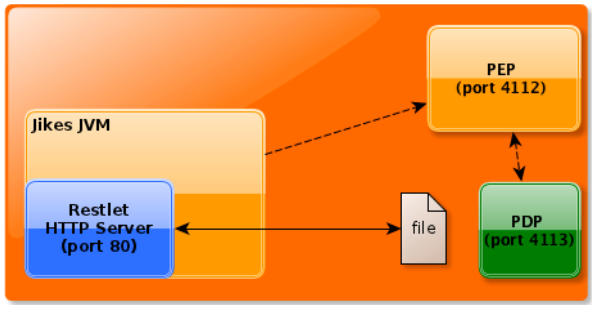

Figure 3. BonFIRE Compute Resource with integrated PEP module

B. *Case-2: When PEP module lies outside server node*

In this set-up, the server nodes are similar to the case-1, but the PEP module is hosted in an external VM. Requests to the external PEP module are triggered over the network. This scheme might result in some performance degradations. ExSec experiment aims to measure the impact of using external PEP on the functioning of security policy enforcement. The architectural set-up is shown in the Figure 4.

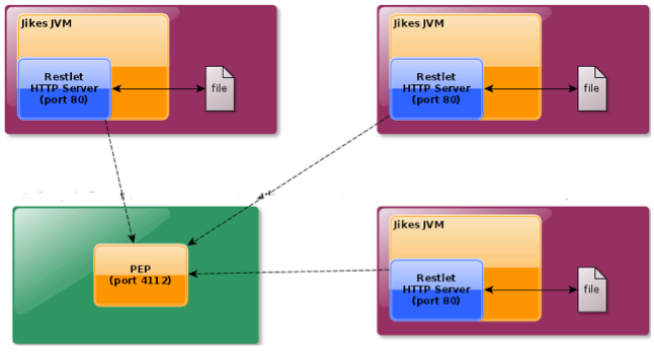

Figure 4. BonFIRE Compute Resource with external PEP module

C. *Testing scenarios*

This section outlines the set of scenarios of ExSec experiment to study the impact of security.

1) *Basic test scenarios*

First we deployed a basic test scenario where only two VMs are used. One contains a server node configuration with an integrated PEP module; and the other performs download request to the first one. We use *HAProxy* load-testing tool to generate large numbers of HTTP client requests to simulate multiple clients. The behavior of the server node is analyzed according to the number of client requests it serves. This scenario is shown in the Figure 5. This test is designed to study the impact of a sizable number of clients' requests on the infrastructure performance.

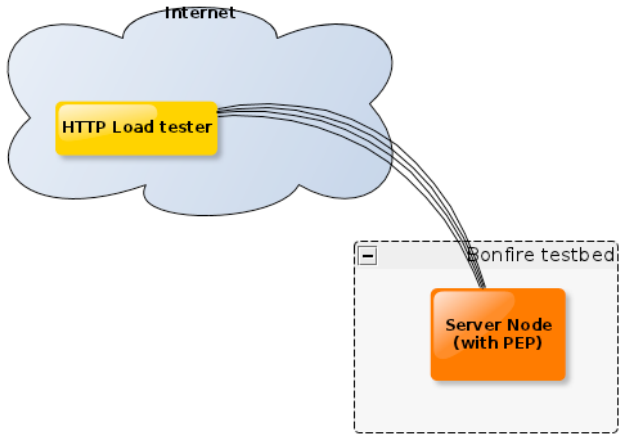

Figure 5. Basic load testing scenario for BonFIRE testbed

2) *Load testing scenario (integrated PEP modules in servers)*

This scenario, as shown in the Figure 6, is meant to analyze the system behavior when multiple client requests are distributed across several server nodes. These could be spread across various BonFIRE testbeds. In this scenario, the PEP modules are integrated into the server nodes. Synchronization of different PEPs can incur some performance overheads. We workout the impact on performance due to increasing load and management overheads.

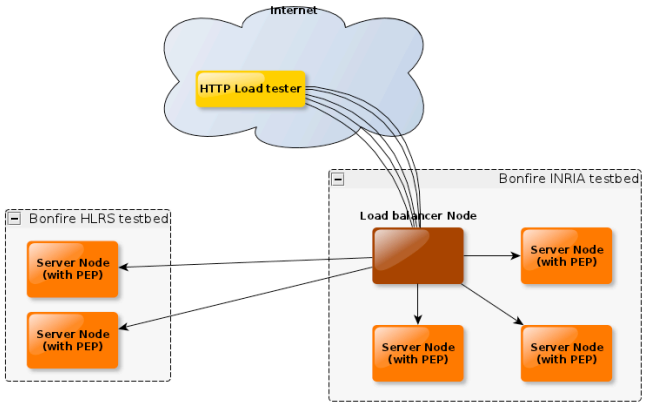

Figure 6. Load testing scenario with integrated PEP module

 ISBN: 978-1-61208-209-7

3) Load testing scenario (one PEP module per BonFIRE site)

This scenario is similar to the previous one, but server nodes are no longer hosting the PEP modules. They are externalized on separate computing resources. However, this scenario provides one PEP module per BonFIRE testbed. This scheme is shown in Figure 7.

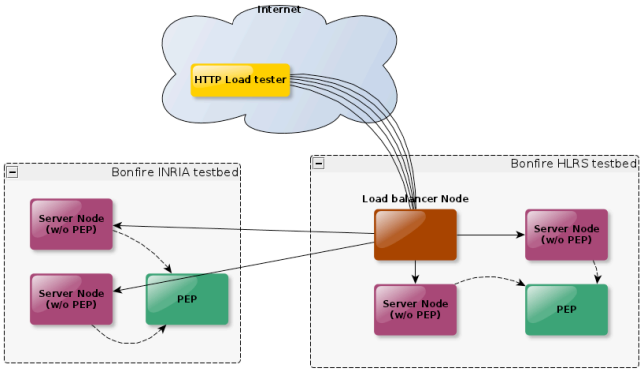

Figure 7. Load testing scenario with one PEP module per BonFIRE site

4) Load testing scenario (one PEP module for the entire infrastructure)

This is a similar scenario as the previous one. However there is only one PEP module, so that server nodes will have to perform Usage Control policy requests across BonFIRE sites. This arrangement is shown in the Figure 8. It would be more measurable to have the PEP on an independent node without server node on it.

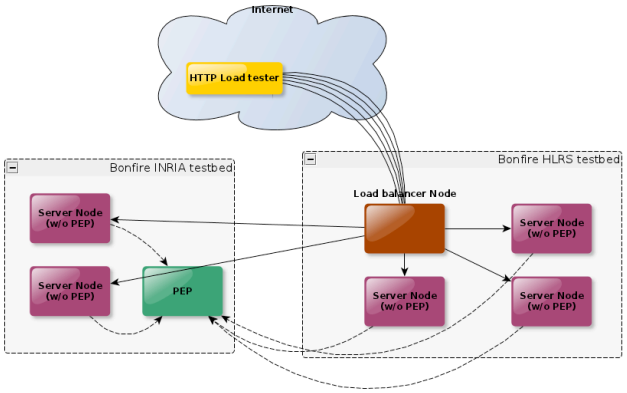

Figure 8. Load testing scenario with one PEP module

V. DISCUSSIONS

Impact on security functions of the wireless devices and platforms is widely explored [17][18][19], mainly due to their significance on the power consumption. The principal objective of these studies is pointed towards improving the battery life of wireless devices instead of investigating the impact on the global functioning of the resources. Whereas, ExSec is aiming to quantify the impact on security performance by studying the impact of its different parameters.

Impact of security services in a client/server exchange of information is evaluated in [20]. The composition of these environments is generally fixed and investigation of the impact of security services on the performance requires less parameters compared to virtual, dynamic and decentralized environments such as federated Clouds. Heterogeneity besides scalability is a non-trivial challenge that we are facing in ExSec experiment. The dynamic nature of the distributed systems is giving rise to *adaptive* security monitoring systems [21]. The decision making process for their adaptiveness also inflicts performance overheads. However, this performance factor is not considered in our work.

Hardware-based security solutions such as *Trusted Computing* [22] are often seen as rigorous in quality of protection. This inspiration has led to the development of hardware-based process security monitoring system such as VMInsight [23] that can provide load-time and run-time monitoring for processes. It can be an interesting follow-up direction for the ExSec experiment; however, the current BonFIRE infrastructure has no Trusted Platform Module (TPM) support. We can nevertheless envision extrapolating ExSec results on some Cloud infrastructure with TPM such as *CertiCloud* [24].

Our work mainly deals with infrastructural side of the performance impact on security. The results can be used to advise Cloud customers and users on the security and performance tradeoffs. However, infrastructure providers (such as Amazon EC2 [25]) do not take responsibility of ensuring protection of their customers' contents. For example, clause 4.2 of Amazon's Customer Agreement explicitly ask their customers to be responsible for taking necessary security measures. It clearly states: *You are responsible for ... taking your own steps to maintain appropriate security and protection, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content*. Likewise, a recent study of *Security of Cloud Computing Providers* [26] reported that around three quarters (73% of US and 75% of European service providers) responded that their cloud services do not substantially protect and secure their customers' confidential or sensitive information. Moreover, nearly two-thirds of the responded (62% of US and 63% of European providers) were not confident that their Cloud applications and resources were secure. It is therefore necessary for the Cloud customers to enforce their security policy and to ensure that its impact on performance remains within acceptable range. Our work can be useful for this kind of public. They can use it together with some trust establishing mechanism for choosing the most appropriate Cloud provider. Example of trust establishing mechanism includes *privacy penetration testing* [27].

 ISBN: 978-1-61208-209-7

VI. CONCLUSIONS AND FUTURE DIRECTIONS

This paper presented our experimental investigations that aim to relate two peculiar characteristics of highly available systems - scalability and heterogeneity - with the performance of security functions. We are working to develop a formal way of quantifying the impact on security services under various operating conditions and parameters of federated Cloud deployments. We as a technology transfer centre perform this experimental study to help businesses (especially SMEs) identify the best security architecture that will fit their Cloud architectures and performance requirements.

Our study is a pioneer work in analyzing the impact of the peculiar characteristics of hybrid Cloud architectures on the much-needed effective security solutions. We are conducting this experimental study on a real life operational hybrid Cloud infrastructure through a set of test scenarios depicting real-life situations of routine business environments. Our work will also stimulate new research directions in the area of Cloud security and its performance parameters; as the security solutions of the pre-Cloud era may not be simply ported to this novel paradigm without necessary improvements.

We are currently implementing usage control (UCON) security policy. Our future directions include implementation of more complex policy rules to better reflect the emerging security requirements. Examples include security policy rules for *reputation* component that grants or denies usage requests according to the client's reputation. We plan to explore such new policies to broaden the scope of the ExSec experiment beyond the single experimentation policy. We are also going to explore ways of compensating performance degradation by making use of available Cloud resources to fill the gap.

ACKNOWLEDGMENT

The research leading to the results presented in this paper has received funding from the European Union's seventh framework programme (FP7 2007-2013) Project BonFIRE under grant agreement number 257386. Authors would also like to express their gratitude to Damien Hubaux and Florian Schreiner who have provided their valuable help in conducting the ExSec experiment.

REFERENCES

[1] Data Center Post, How Network Performance and Security Monitoring are Useful in Today's Data Center, online article at Technorati.com, 26 April 2011 [retrieved: June 2012]

[2] W. Jansen, Directions in Security Metrics Research, NIST Interagency/Internal Report (IR) no. 7564, March 2009 [retrieved: June 2012]

[3] Cisco product: Security Monitoring, Analysis and Response System (MARS) [retrieved: June 2012]

[4] Hewlett Packard (HP) product: IT Performance Suite [retrieved: June 2012]

[5] J.M. Cary, Data security and performance overhead in a distributed architecture system, UMI Research Press, 1981 [retrieved: June 2012]

[6] European 7th Framework project BonFIRE: Building Service Testbeds on FIRE (Future Internet Research Experimentation)

[7] S. Naqvi and P. Mori, Security and Trust Management for Virtual Organizations: GridTrust Approach, IFIP International Conference on Trust Management (IFIPTM'09), West Lafayette, USA, June 2009

[8] European 7th Framework project RESERVOIR: Resources and Services Virtualization without Barriers

[9] The OpenNebula Cloud Management Engine [retrieved: June 2012]

[10] The ZABBIX Performance Monitoring Tool - www.zabbix.com

[11] Restfully: A general-purpose client library for RESTful APIs [retrieved: June 2012]

[12] The JavaScript Object Notation (JSON) data-interchange format [retrieved: June 2012]

[13] A.S. Ibrahim, J.H. Hamlyn-Harris, J. Grundy, and M. Almorsy, CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model, in proceedings of the 5th International Conference on Network and System Security (NSS), 2011, pp.113-120, 6-8 September 2011, Milan, Italy, ISBN: 978-1-4577-0458-1

[14] T. Garfinkel, and M. Rosenblum, A Virtual Machine Introspection Based Architecture for Intrusion Detection, in proceedings of the 10th Network and Distributed Systems Security Symposium (NDSS) 2003, pp 191-206, 6-7 February 2003, San Diego, CA, USA

[15] F. Van Staden, and H. Venter, Adding digital forensic readiness to electronic communication using a security monitoring tool, in proceedings of the IEEE Information Security South Africa (ISSA) 2011, 15-17 August 2011, Johannesburg, South Africa

[16] OASIS Extensible Access Control Markup Language (XACML)

[17] S. Kolahi, Z. Qu, B. Soorty, N. Chand, The Impact of Security on the Performance of IPv4 and IPv6 Using 802.11n Wireless LAN, in Proceeding of the 3rd International Conference on New Technologies, Mobility and Security 2009 (NTMS 2009), 20-23 December 2009, Cairo, Egypt, ISBN: 978-1-4244-4765-7

[18] J. Schonwalder and V. Marinov, On the Impact of Security Protocols on the Performance of SNMP, IEEE Transactions on Network and Service Management, pp.52-64, Vol. 8, Issue 1, 2011

[19] A. K. Agarwal and W. Wang, Measuring performance impact of security protocols in wireless local area networks, in Proceedings of the 2nd IEEE International Conference on Broadband Networks 2005 (BroadNets 2005), 3-7 October 2005, Boston, MA, USA

[20] S. Cavalieri, G. Cutuli, S. Monteleone, Evaluating impact of security on OPC UA performance, 3rd IEEE Conference on Human System Interactions 2010 (HSI 2010), 13-15 May 2010, Rzeszow, Poland

[21] R. Savola and P. Heinonen, Security-Measurability-Enhancing Mechanisms for a Distributed Adaptive Security Monitoring System, in proceedings of the Fourth International Conference on Emerging Security Information, Systems and Technologies 2010 (SECURWARE'10), 18-25 July 2010, Venice, Italy

[22] The Trusted Computing Group technologies [retrieved: June 2012]

[23] X. Li, C. Jiang, J. Li, B. Li, VMInsight: Hardware Virtualization-Based Process Security Monitoring System, in Proceedings of the IEEE Int. Conference on Network Computing and Information Security 2011 (NCIS 2011), 14-15 May 2011, Guilin, China

[24] B. Bertholon, S. Varrette, and P. Bouvry, CertiCloud: A Novel TPM-based Approach to Ensure Cloud IaaS Security, in Proceedings of the 4th IEEE International Conference on Cloud Computing 2011 (CLOUD 2011), 4-9 July 2011, Washington DC, USA

[25] Amazon Elastic Compute Cloud (Amazon EC2)

[26] Ponemon Institute study (sponsored by CA Technologies), Security of Cloud Computing Providers Study, April 2011 [retrieved: June 2012]

[27] C. Probst, A. Sasse, W. Pieters, T. Dimkov, E. Luysterborg, and M. Arnaud, Privacy penetration testing: How to establish trust in your Cloud provider, In: European Data Protection - In Good Health? S. Gutwirth, R. Leenes, P. De Hert, Y. Poullet (Eds.), 2012

 ISBN: 978-1-61208-209-7