Performance Analysis of a Two Stage Security Approach in Cloud Computing

Conference Paper · June 2015

CITATIONS
0

READS
66

1 author:

Hassan el ghazi
Institut National des Postes et Télécommunications
57 PUBLICATIONS **209** CITATIONS

SEE PROFILE

Performance Analysis of a Two Stage Security Approach in Cloud Computing

Mehdi EZZARII*,
Institut National des Postes et Télécomunications (INPT),
Rabat, Morocco
ezzarii.mehdi@gmail.com

Hassan EL GHAZI,
Institut National des Postes et Télécomunications (INPT),
Rabat, Morocco
h.elghazi80@gmail.com

Hamid ELGHAZI, Tayeb SADIKI,
Université International de Rabat (UIR)
Rabat, Morocco
{hamid.elghazi; tayeb.sadiki}@uir.ac.ma

Abstract—**Cloud computing is emerging as a promising IT paradigm. Many challenges are still hanging ahead for the Cloud to jump into the maturity stage. Thus, security is deemed as a main challenge. In this paper, we develop the performance of intrusion detection solutions (IDS) by analyzing their performance in terms of recognition, security and capacity. The main aim of our work is to help engineers to implement adequate solution (IDS) depending on the security levels of cloud computing. Our proposed method is based on two-stage. The first stage consists on studying the needed requirements of IDS solution in cloud computing. The second stage classifies security attacks based on four levels. The classification identifies attacks that we should treated with the fitting solution.**

Keyword:Cloud Computing; Security; IDS; Requirements;Architecture levels.

I. INTRODUCTION

Cloud Computing provide computing as a utility. It shifts Computing from being a mere product to become a utility like electricity, water, and telephony.

From time to another, computing is becoming ubiquitous (all is needed is a socket) and the payment method is a pay-per-use one, i.e., the consumer pays for only what he used exactly like electricity, water and telephone expenses. However, a couple of challenges are still posed ahead for the technology to reach the maturity stage, e.g., privacy and security.

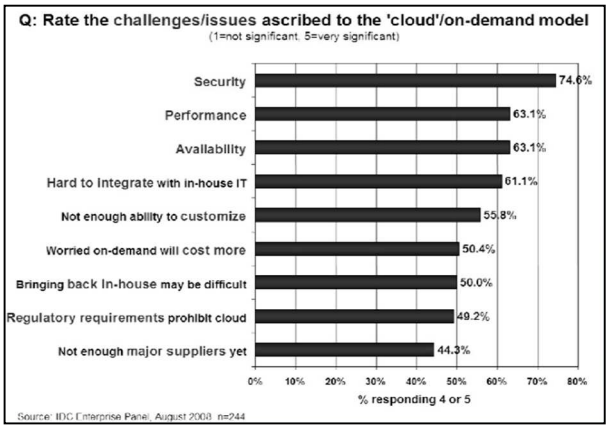

Figure 1. Challenges/issues ascribed to the Cloud computing (Source: IDC report 2008)

In this work, we address the security aspect in cloud computing to find efficient solutions to protect this kind of environment. Moreover, by solving the issue of security the usage of Cloud Computing area will grow quickly.

We believe that security issues in cloud computing are related at first to intrusion attacks. Vulnerability problems in cloud computing security systems are inherent essentially from not detecting unwanted users. In this paper, we analyze intrusion attacks from the performance point view. Because, in Cloud Computing the security solutions take into account not only the completeness of the security algorithm but also other constraints such as: Resource Pooling, Rapid elasticity, Measured Service, On-demand self-service and broad network access [1].

If the relationship between the technical security solution and the needed security performance is identified early, the resulting approach could be powerful.

The proposed approach in this article focus on this relationship by using a performance oriented analysis of the security issues in cloud computing.

First, we start by identifying the needed requirements of a security system in cloud computing area. The resulting requirements are analyzed at first from a performance point of view.

Our approach introduces a new level-classification structure to organize security solutions from external to internal treatments. We use classification to analyze existing security solutions into four levels.

These classifications will help security engineers later in the task of defining adequate security architecture for the corresponding Cloud Computing environment. Thereby, engineers will be able to propose the correct response to security attacks.

Finally, we will apply our proposed method in the context of IDS attacks as a case study.

II. OVERVIEW OF TWO-STAGE APPROACH NETWORK

The first stage consists of providing a performance oriented analysis to describe and identify the needed security requirements and performances of a Cloud Computing environment.

At this stage, we define indicators and performance metrics of security taking into account the requirements of the cloud-computing environment.

This stage gives engineers of security the prerequisites and indicators related to cloud computing environment in face. Then, it helps them aware of the security level that shall be taken into account according to the characteristics of the faced cloud computing environment.

The second stage concerns the evaluation of the different security techniques and solutions related to the expected performance. The resulting evaluation is based on the treatments classification mechanism to help engineers to build the security levels of solutions. We will demonstrate the utility of using levels analysis mechanism in Intrusion Detection context. Thereby, the security engineer could choose the best intrusion security solutions from many options.

III. Performance Analysis in Cloud Environment– Stage One

We have studied the main characteristic of cloud computing environment in comparison with a classic network. We found five main features/characteristics [2] impacting directly the security performance: Resource Pooling, Rapid elasticity, Measured Service, On-demand self-service and Broad Network Access.

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multitenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned in some cases automatically to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts).

On-demand self-service: A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically without requiring human interaction with a service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.

The table below illustrates the relation between cloud features/characteristic and the security issues related to each one.

TABLE I. Security Aspect cloud computing

Cloud Characteristic	Security Aspect[3]
Resource pooling	Secure Virtualization, Flexibility of adapting the security solution, High rate of dettection of anomalies and intrusions in VM, Storage problems
Rapid elasticity	Multi-tenancy, Computational cost and complexity of security solution method have to be low. Capability to protect and analyze the high speed trafic
Measured service	Service Level Agreement, Extensibility and Shared Responsibility
On-demand self-service	Service Level Agreement, Extensibility and Shared Responsibility, Capability to include the detection meccanism of attacks and intrusions in real time.
Broad network access	Heterogeneity, Outsourcing, capability of secuity solution to detect all types of attacks and intrusion related to différents platform and profils.

Based on this table we will develop the key performance indicators to analyze and measure the satisfactory of security requirements. Furthermore, we analyze the degree (positively or negatively) of impact of a security solutions in the cloud-computing environment such as the ability to detect attacks, processing performance and integrating heterogeneous solutions. The table below illustrates an example of performance metrics.

TABLE II. Performance metrics

Performance	Metrics	Security Solutions
Category	Features	Features Values

The key performance and the impact analyses will be presented with details in the case study section.

IV. Cloud Computing Classification Levels – Stage two

The second stage of our approach is based on the identification of a new structure of security classification. Our approach completes the classical cloud computing structure based on three layers: IaaS, PaaS and SaaS [4].

- Software as a service (SaaS): is any application or software that is running on the platform of the cloud provider, it is a service with access by permission. To access you can use a light client (for example: web browser) to send data a receive results. In addition the consumer has limited authority because he has the right to set up certain parameters so that it has no knowledge on the infrastructure used by the provider of the cloud.
- Platform as a service (PaaS): in this service model, the service provider provides basic accessories, which includes the operating system, network, servers, and development tools that allow different users this service to develop their applications.
- Infrastructure as a service (IaaS): in cases where a user of cloud computing has developed its own applications and he needs just to the hardware infrastructure to deploy. The service provider offers

a complete infrastructure on demand with different components (processors, network, storage, etc.)

Our classification organize all security attacks based on their sensitivity levels in a cloud computing network (see Fig.2).

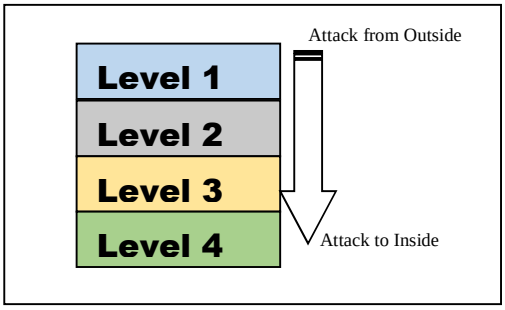

Figure 2. Levels of security concerns

Level 1: in Frontend of cloud architecture: Front-end is the side that is visible for the client, customer or the user. It includes the client's computer system or network that is used for accessing the cloud system. Different Cloud Computing system has different user interfaces. At this level, the security will focuses on protection of application level traffic.

Level 2: in Backend of cloud architecture: Back-end is the side used by the service provider. It includes various servers, computers, data storage systems etc. that builds together the cloud of computing services. This system can include different types of computer programs. The security will focuses on protection of traffic inter-VM and inter-Server.

Level 3: in Hypervisor for virtualization level: The hypervisor supports hardware-level virtualization on bare-metal devices like CPU, memory, disk and network interfaces. The hypervisor software sits directly between the physical hardware and the OS. This virtualization layer is referred to as either the VMM (Virtual Machine Monitor) or the hypervisor.

In this level, security should be focused in inter-VM traffic and face to intrusions and attacks go at bare-metal devices (CPU, memory, disk and network interface...).

Level 4: in each Virtual Machine: A VM was originally defined by Popek and Goldberg as "an efficient, isolated duplicate of a real machine". A virtual machine provides a complete system platform which supports the execution of a complete operating system (OS) and Applications. In this level, security will focuses on the protection against attacks specifically related to this VM environment as listed in the beginning of the article.

The table 3 gives a classification of security levels per Cloud level. The table also gives information about the expected intrusions attacks corresponding to each level [5].

TABLE III. CLASSIFICATION OF SECURITY LEVELS IN CLOUD COMPUTING

Architecture levels			**Performance Classification**	**Type of attacks and intrusions**
IaaS	***SaaS***		Level 1 : in Frontend of cloud architecture	a) External intrusion b) Attempted break-ins, which are detected by a typical behavior profiles or violations of security constraints. c) Malicious use, which is detected by a typical behavior profiles, violations of security constraints, or use of special privileges.
IaaS	***PaaS***		Level 2 : in Backend of cloud architecture	a) Internal intrusion b) Masquerade attacks, which are detected by a typical behavior profiles or violations of security constraints. c) Flooding attack :DoS & DDoS d) Port scanning: provides list of open ports.
IaaS	***PaaS***		Level 3 : in Hypervisor for virtualization level	a) Penetration of the security control system, which are detected by monitoring for specific patterns of activity. b) Attacks on virtual machine (VM) or hypervisor: Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.
IaaS	***PaaS***	***SaaS***	Level 4 : in each Virtual Machine	a) Leakage, which is detected by a typical use of system resources. b) Denial of service, which is detected by a typical use of system resources. c) Insider attack: Disclose or modify information intentionally

We can conclude through the table 3 that comprehensive security solution in the cloud computing must consider the needs of different levels from 1 to 4 in cloud computing.

V. THE TWO STAGE APPROACH FOR INTRUSION DETECTION SYSTEM (IDS) SOLUTION

A. *Introduction to IDS solution*

1) IDS

Intrusion detection systems are software or hardware systems that automates the process of monitoring the events occurring in a computer system or network, analyzes them for malicious activities or policy violations and produces reports to a management station [6].

This system includes a set of information used to detect intrusions in a kind of knowledge base attack, for example the configuration information of the current system status and information audit of writing events that occur on the system.

An IDS is composed of several components [7]:

- Sensors which generate security events.
- Console to monitor events and alerts and control the sensors.

- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

2) Technique of IDS solution

Signature based detection: Signature based intrusion detection technique can be used to detect known attack. It identifies intrusion by matching captured patterns with preconfigured knowledge base. It can be used either at front-end of Cloud to detect external intrusions or at back end of Cloud to detect external/internal intrusions [5].

Anomaly detection: Anomaly (or behavioral) detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior. Anomaly based approach involves the collection of data relating to the behavior of legitimate users over a period of time, and then apply statistical tests to the observed behavior, which determines whether that behavior is legitimate or not [5].

Other techniques of detection: There are many soft computing techniques such as Artificial Neural Net- work (ANN) (Han and Kamber, 2006), Fuzzy logic (Han and Kamber, 2006), Association rule mining, Support Vector Machine (SVM) ((Han and Kamber, 2006), Genetic Algorithm (GA) (Dhanalakshmi and Ramesh Babu, 2008; Li, 2004), etc. that can be used to improve detection accuracy and efficiency of signature based IDS or anomaly detection based IDS [5].

B. Performance Analysis of IDS – Stage One

We detail in the following section for each IDS techniques listed in table 4 some performances related to detection in term of performance of detection, recognition and analysis capacity.

1) Criteria and metrics performances of IDS solution

Metrics and performances characteristics of a number of techniques and methods of IDS solution are numerous and can be defined in several ways according to the constraints and conditions environments where IDS is installed.

TABLE IV. CRITERIA AND METRICS PERFORMANCES OF IDS TECHNIQUES

Category	Metric	IDS technique							
		T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**
		Signature based detection (snort-based IDS/traditio nal algo matching)	***Anomaly detection***	***Artificial neural network (ANN) based IDS***	***Fuzzy logic based IDS***	***Association rule based IDS***	***Support vector machine (SVM) based IDS***	***Genetic algorithm (GA) based IDS***	***Hybrid techniques***
Recognition capability	Dr	Medium	High	Medium	High	Medium	High	Medium	High
	Fp	High	Low	Medium	Low+	Low	Low+	Medium	Low
	Fa	High	Low	Medium	Low	Low	Low	Medium	Low
	Da	Low	High	High	Medium	Medium	High	High	High
Detection Performance	Cc	Medium	High	High	High	Medium	Medium	Medium	High+
	Ak	1	0	0	0	1	0	0	1
	Au	0	1	1	1	0	1	1	1
	Ru	High	High+	Medium	Medium	Medium	Low	Medium	High
	Cx	0	1	1	1	1	1	1	1
Performance Analysis	Hs-Pd	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Hs-Pa	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Hv-Pd	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Hv-Pa	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium

Below a short description of the performances and characteristics and metrics according to our approach. The metrics are grouped according to the following categories:

Recognisation capability Category the ability of the technique or method of IDS to provide a good recognition mechanisms of security in the network or at the end points. In this category, we can define the following metrics:

- Detection Rate (Dr) is the rate of correctly detecting the abnormality compared to the total anomaly occurs in the target network. For best performance, Dr Rate should be high [8].
- Detection Accuracy (Da) is the rate to have an accuracy of detection of the anomaly and like whatever the detected anomaly really is an anomaly. For best performance, Da Rate should be high.
- False Positive (Fp) is an error in judgment of a detection of an abnormality that is not. For best performance, the Fp value should be low [8].

- False Alarm (Fa) is the generation rate of false alarm of an abnormality that is not. For best performance, the Fp value should be low [8].

We give the values High, Medium and Low for each metric included in this category to evaluate each IDS method of our comparative study.

We can also add both (Ak) and (Au) characteristics in this category which respectively represent the capacity of the IDS method to detect a known attack (valeur'1 'or ' 0 ') and the ability to detect an unknown attack (valeur'1' or '0').

The detection performance category takes into account the complexity of the treatment process, the cost of computation and the performance of the resources used. In this category, we can define the following metrics:

- Computational cost (Cc) is the cost calculation processing of the detection method. For best performance, we always try to have a low cost of computing.
- Complexity (Cx) represents the complexity of the method used from the functions used (linear or non-linear, structured data and unstructured ...). For our comparative study, we give the values '1' if it is complicated if not '0'.
- Resource use (Ru) is the resource consumption rates for the implementation of these techniques in terms of CPU load, memory ... the best performance of the IDS technique lies in the optimization of resource consumption. For our comparative study, we give the values '1' if there are fewer consumable resources otherwise the value '0'.

The evaluation of the performance of these IDS methods can also be based on the traffic analysis capabilities across multiple dimensions. We then define the *performance analysis category* by taking measures the following metrics:

- High-speed traffic (Hs) which consists in the ability to analyze a high value traffic over time and we can measure this metric by Dropped packet rate (Hs-Pd) and by packet rates analyzed (Hs-Pd).
- Heavy traffic (Hv), which involves the ability to analyze heavy traffic and we can measure this metric as the Dropped packet rate (Hs-Pd) and packet rates analyzed (Hs-Pd) [9].

With these two metrics, the performance will depend on the rate: if the rate of dropped packets is small or the rate of the analyzed packets is large.

2) Levels Analysis of IDS Solutions – Stage Two

Based on the results of the performance analysis stage, we can propose a new kind of architecture based on the levels analysis proposed by our approach. The levels analysis drive engineers to organize the location of different IDS solutions in the cloud by consider the following conditions:

- At *Frontend level*, we can place the IDS1 type use as a combination of technical IDS T1 and T3 because the traffic is less. At this level, the required performance is related to kind of recognition for high protection against external attacks. Also it does not require a high value of the analysis performance since the traffic is not voluminous.
- At *Backend level*, the traffic is heavy as it may be some inter-server traffic. At this level we put the IDS2 type using IDS solutions T1, T4 and T6. This site requires a high-performance analysis and an important traffic criteria Hv-Pd and Hv-Pa. The IDS2 must also have a high-performance detection performance category essentially minimizing the execution time of the techniques used and the resources consumed.

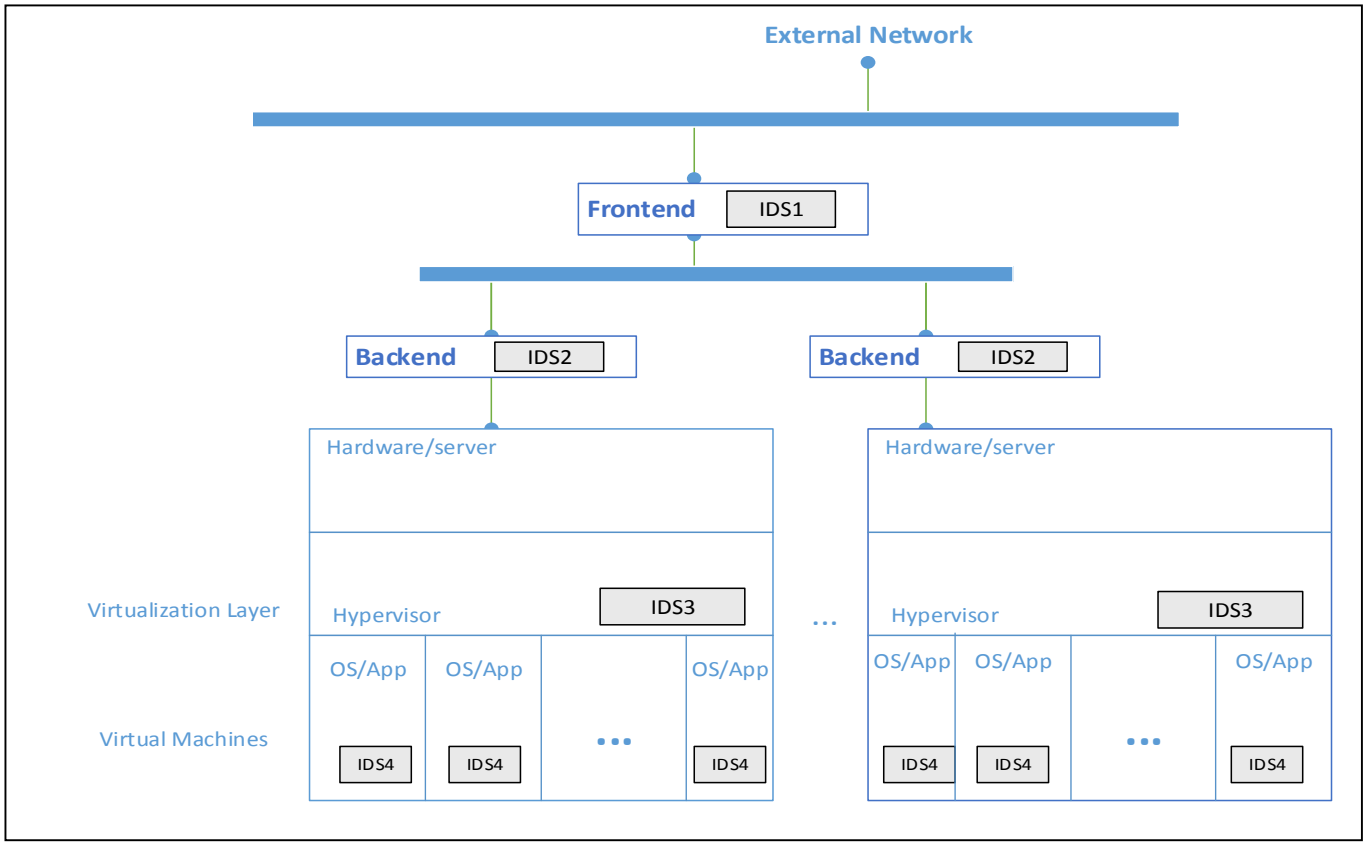

Figure 3. Classification of different IDS solutions in Cloud computing

- At *the hypervisor level*, the IDS3 will analyze inter-VM traffic and at the same time the contents of the hypervisor. It shall be composed of T6 and T7 IDS techniques because this level requires a high performance detection and security.
- At *virtual machines level*, we will place the type IDS4 as host-IDS. We choose to use T2 or T4 techniques to have a high performance in terms of accuracy detection.

The matrix below resume the level analysis process of IDS solution. The matrix show the corresponding level for each solution.

TABLE V. SOLUTION AND IDS TECHNIQUES MATRIX

		T1	T2	T3	T4	T5	T6	T7
L1	*IDS1*	●		●				
L2	*IDS2*	●			●		●	
L3	*IDS3*						●	●
L4	*IDS4*		●		●			

The most used IDS techniques are those listed in the matrix below. The comparative study are based on criteria such as the best rate of intrusion detection and accuracy of detecting attacks (known or unknown).

At the end of this work, engineers can identify the right solution of the security problems in the context of cloud computing. They will be sure that there architecture satisfy both security and the performance concerns.

VI. CONCLUSION

In this work, we tried to detail our approach based on two important steps: stating the requirements needed of a security system in cloud computing. And then presenting four levels which classify security attacks. We applied then our approach to IDS attacks.

Our future contribution will focus on detailing the process of matching requirements to architectures in the cloud environment. We will looking in next work to the evaluation of the performance of our approach.

REFERENCES

[1] Anthony T. Velte, Toby J. Velte, Ph.D. Robert Elsenpeter. Cloud Computing: A Practical Approach. E-Book

[2] F. Shahzad “State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions” The 6th International Symposium on

Applications of Ad hoc and Sensor Networks (AASNET'14)

[3] Takabi, H., Joshi, J., Ahn, G.J. Securecloud: Towards a comprehensive security framework for cloud computing environments.In: Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual. 2010, p. 393–398

[4] J. Che, Y. Duan, T. Zhang, J. Fan "Study on the security models and strategies of cloud computing". 2011 International Conference on Power Electronics and Engineering Application - 2011.

[5] C. Modi, D. Patel a, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan "A survey of intrusion detection techniques in Cloud". Elsevier Journal ofNetworkandComputerApplications36(2013)42–57

[6] A. Zarrabi, A. Zarrabi "Internet Intrusion Detection System Service in a Cloud". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012

[7] V. Marinova-Boncheva, "A short survey of intrusion detection systems," Problems of Engineering Cybernetics and Robotics, vol. 58, pp. 23–30, 2007

[8] H.H. Soliman, N. A. Hikal, N. A. Sakr, "A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks", Egyptian Informatics Journal (2012) 13, 225–238

[9] W. Bul'ajoul, A. James, M. Pannu "Improving network intrusion detection system performance through quality of service configuration and parallel technology" J. Comput. Syst. Sci. (2015)