Node Verification to Join the Cloud Environment Using Third Party Verification Server

https://doi.org/10.3991/ijim.v11i4.6501

Ashraf H. Aljammal*
The Hashemite University, Zarqa, Jordan
ashrafj@hu.edu.jo

Hani Bani-Salameh
The Hashemite University, Zarqa, Jordan
hani@hu.edu.jo

Ayoub Alsarhan
The Hashemite University, Zarqa, Jordan
ayoubm@hu.edu.jo

Mohammad Kharabsheh
The Hashemite University, Zarqa, Jordan
mohkh86@hu.edu.jo

Mamoon Obiedat
The Hashemite University, Zarqa, Jordan
mamoon@hu.edu.jo

Abstract—Currently, cloud computing is facing different types of threats whether from inside or outside its environment. This may cause cloud to be crashed or at least unable to provide services to the requests made by clients. In this paper, a new technique is proposed to make sure that the new node which asks to join the cloud is not composing a threat on the cloud environment. Our new technique checks the node before it will be guaranteed to join the cloud whether it runs malwares or software that could be used to launch an attack. In this way the cloud will allow only the clean node to join it, eliminating the risk of some types of threats that could be caused by infected nodes.

Keywords—Cloud computing, Cloud security, Network security, Node scanning.

1 Introduction

Cloud computing is considered the phenomena of the century, as it provides different types of supports/services to the organizations as a software manifestation [1-3]. A three types of services could be provided by the cloud providers; Software as a service SaaS, platform as a service PaaS and infrastructure as a service IaaS[4-6].More about the cloud services is discussed in section 2.

Nowadays, cloud environment witnesses a different types of threats and attacks which targeting its infrastructure including the virtual machines and the supported softwares as well as the clients/users data [7-11]. Therefore, different security measures had been implemented in the cloud environment such as firewalls, IDS and IPS as a try to secure it [12]. However, the used security measures are still insufficient to secure the cloud environment as the number of attacks is increasing[13]. In addition, it focuses on the cloud environment and the clients who are already connected to the cloud neglecting checking the clients for security threats before joining the cloud.

On the other hand, the availability of the cloud environment is considered one of the most important challenges the cloud providers face since the cloud concept had been introduced [14, 15]. Where, the cloud service providers should have a balance between the availability of the cloud services and the security measures they use.

As most of the used security measures in the cloud tries whether to detect or prevent attacks of the nodes that are connected to the cloud environment; The previously unknown security related information about the nodes that request to join the cloud environment may compose a threat on the cloud environment components[14]. Therefore, a prior collection of security related information about the node will help the cloud to make decision of allowing the node to join the cloud or not.

If the cloud could have a prior security related information, it will be able to decide whether the node which requested to join the cloud composes a threat on the cloud environment components or not. The node could be whether infected by a malware or running software that may be used to launch some types of attacks. In addition, the attacker who wants to launch an attack needs to run some attack tools on his/her machine. Therefore, if we could detect these hacking tools and malwares remotely before launching the attack, then we can prevent this attacker from entering the target cloud and causes troubles.

Thus, many security concerns should be highlighted regarding adding new nodes to cloud. Therefore, adding new node to the cloud environment shouldn't be On-The-Fly step. Each node should be verified and checked before it got trusted to join the cloud environment[16].

As a result, if the cloud could be able to make a decision to allow or forbid the node from joining the cloud, then the risk of adding new node to the cloud that may compose a security threat will be decreased.

2 Cloud Computing Architecture

The NIST has defined the cloud as an on demand model that enables client/users to access a shared pool of customized computing resources minimizing the management efforts of the provided resources[17].

Based on the NIST definition, cloud model is composed of the following components:

2.1 Essential Characteristics

A five essential characteristics and features should be existed in the cloud model to serve its goals. This section introduces a detailed discussion of these characteristics.

- On-demand self-service: Clients can use the provided services of the cloud automatically whilst no need for supervision of the service provider.
- Broad network access. The ability to use the cloud services over network using heterogeneous clients platforms.
- Resource pooling. A pool of resources are provided for multi-clients, such as, processing, memory, or storage. Whilst, the clients has no knowledge of an exact location of the provided resources.
- Rapid elasticity. The ability to accommodate the clients on-demand services rapidly, while the clients feel like the capabilities are unlimited and could be used any time, regardless of the quantity.
- Measured service. The ability to monitor and control the usage of the provided resources by the cloud (i.e. storage) for the purpose of transparency between the provider and the clients.

2.2 Service Models

Following is a discussion of the three service models that are provided by the cloud.

- Software as a Service (SaaS). Is to provide the clients with an applications to be used while it is running on the cloud servers instead of the clients' machines. Thus, the clients have no control over the underlying cloud infrastructure. Google Docs (http://docs.google.com) is an example of the SaaS.
- Platform as a Service (PaaS). The ability of providing the clients with a set of supported programming language to be able to build their own applications.
- Infrastructure as a Service (IaaS). To provide the user with the needed resources to deploy and run their own applications including operating systems. In IaaS, the clients has the ability to access the underlying infrastructure using the virtual machines.

2.3 Deployment Models

A four deployment models are introduced to deploy the cloud environment, following is a detailed discussion of them.

- Private cloud. The cloud is used by a specific users and limited to a particular organization. The cloud owned and managed either by the organization or a third party.
- Community cloud. The community could be a number of different organizations who may share the cloud for a specific purpose. The cloud could be owned by the community, one organization or even owned by a third party.

- Public cloud. It is open for the general public clients and could be owned by any organization (i.e. academic).
- Hybrid cloud. It is a combination of two or more of the aforementioned cloud infrastructures (private, public, or community). And they are bounded together using a suitable technology.

3 Related Work

Many researchers have proposed an IDS techniques to detect intrusions inside the cloud environment. This section discusses some of these techniques.

A real time IDS is proposed by [18] by installing it on a virtual switch inside the cloud environment. The proposed IDS filters the ingoing and the outgoing packets from/to the cloud environment. It uses a predefined rule database for well-known intrusions. The proposed IDS is able to detect intrusions and notify the virtual server to take the correct action based on the attack type.

[8] Have proposed an integrated IDS with cloud environment, by combining the advantages of distributed system and the characteristics of the cloud computing. The proposed technique relies on the snort DB for the purpose of misuse detection. They deployed a network based IDS to observe the network, transport and application layer internal as well as the external activities in the cloud environment.

[19] have proposed a mobile based IDS in the cloud environment by deploying the virtual neighborhood observation. The idea of the proposed technique is to detect the intrusions of the cloud applications and virtual machines that are outside the organization using mobile agents. Therefore, the mobile agents will collect the attack information from the monitored virtual machines for further analysis. Which as a result, introduces more load as the number of virtual machines increases.

A multi-threaded NIDS has been proposed by [20] for a distributed cloud environment. The proposed technique monitors and captures the ingoing and outgoing packets of the types (ICMP, TCP, IP, and UDP). The captured packets will be analyzed against a signature database which contains signatures of a well-known intrusion. The multithread architecture is used to improve the detection performance as the IDS should work as a real time application. Afterward, if an intrusion is detected; the third party monitoring and advisory service will generate a report and alert the cloud service provider.

[21] have introduces an IDS as a service (CIDSS) which is integrated with the cloud environment. The main goal of this serves is to keep the clients secure against attacks that may target the cloud environment. It composed of IDS agents that are integrated in the network segment in addition to a central detection engine which is fed by a group of agents. This as a result, makes it as a distributed structure adapting the scalability of the cloud environment.

An IDS for cloud environment has been proposed by [22]. The proposed technique is composed of four components. The first is the local data collector which collect data from the distributed agents that are located on the network segments. The second is the local analyzer which analysis the collected data by the local data collector, for the purpose of intrusion detection and generating alerts. The remote data collector is the third component which collects the captured data by critical agents and the ones that run security measures. And the fourth component is the cloud computing data center which in turn is composed of Global Analyzer(GA),Network resources collectors(NC),Global Intrusion database(GIDB). This proposed technique suffers from the scalability problem as its performance gets reduced as the cloud environment getting grow.

Finally, the proposed security measures and IDS techniques that deal with the cloud environment are only able to detect the intrusions while they are inside the cloud environment.

4 Proposed Technique

The cloud server has to make sure that the nodes which join the cloud don't compose any threat on the cloud environment. Therefore, our proposed technique aims to check whether the node which asks to join the cloud is clean of attacking tools as well as malwares or not.

As shown in Fig. 1, once the user asks to join the cloud environment, the cloud server will redirect the user to a third-party-verification (TPV) server. Which in turn will scan the user’s machine for any of the malicious softwares including attack tools. If the result shows that the node is clean; then user request will be accepted to join the cloud. Otherwise, the request will be refused because the user’s machine is infected with malicious software. Fig. 2 illustrates the sequence diagram of the proposed technique.

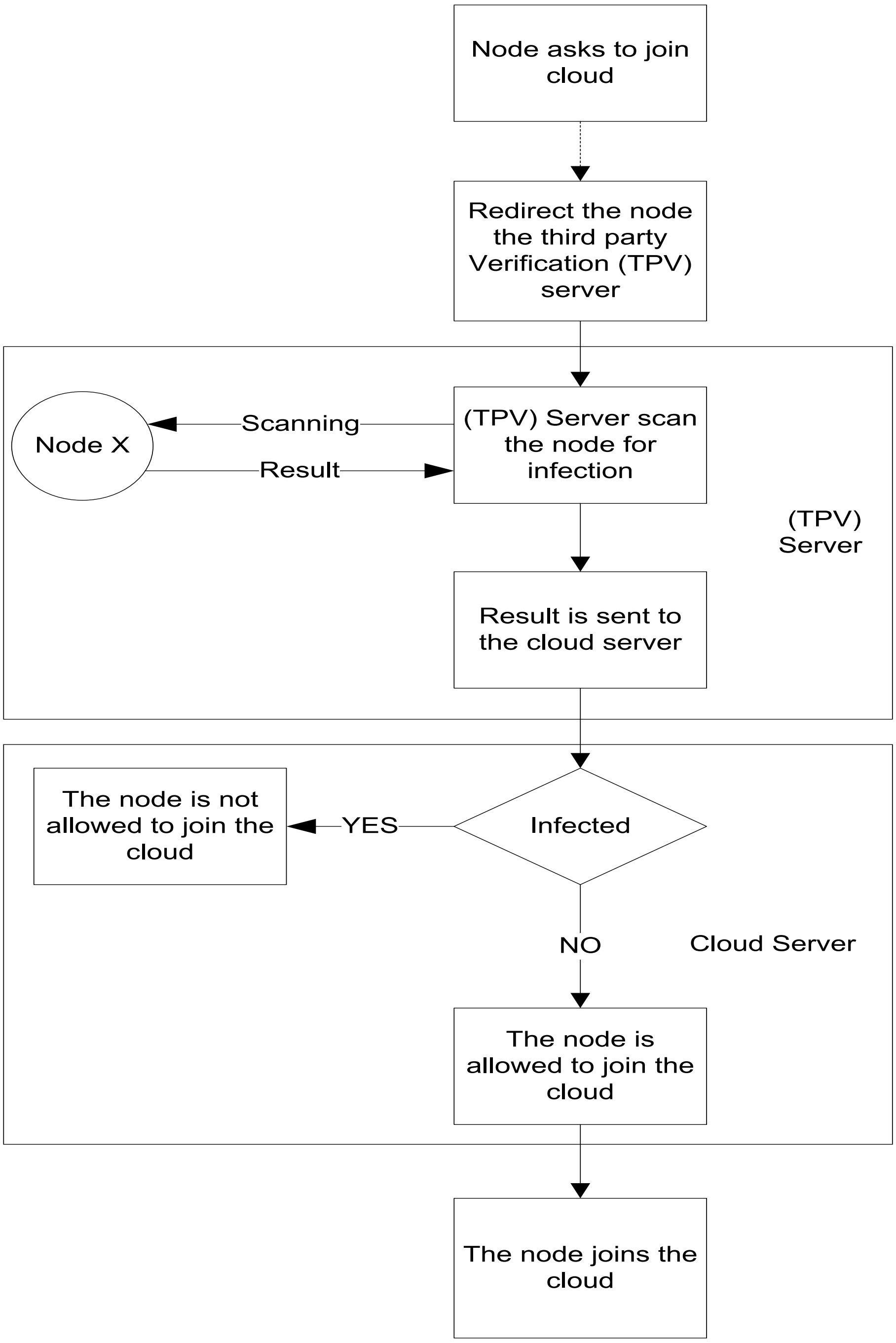
Node asks to join cloud
Redirect the node the third party Verification (TPV) server
Node X
Scanning
Result
(TPV) Server scan the node for infection
(TPV) Server
Result is sent to the cloud server
The node is not allowed to join the cloud
YES
Infected
NO
Cloud Server
The node is allowed to join the cloud
The node joins the cloud

Fig. 1. The proposed technique (NVTPV)

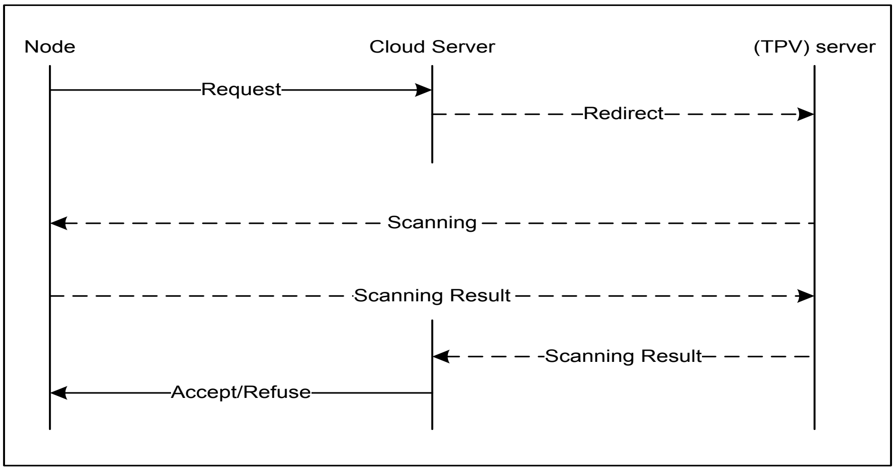

Fig. 2. The sequence diagram of the proposed technique

5 Results and Discussion

In this section, two scenarios will be discussed.

5.1 Scenario #1 A clean node asks to join the cloud environment.

Once the node A asks to join the cloud environment, the cloud server redirected it to the (TPV) server to be scanned for any infection. After the (TPV) server scanned the node A for infection (malware).

The (TPV) server found the target node clean (malware free). Afterward, the result is sent to the cloud server to make the decision and since the result showed that the node A is clean; the cloud will accept the node request to join the cloud as shown in Fig. 3.

5.2 Scenario #2 An infected node asks to join the cloud environment.

As illustrated in Fig. 4, the node B asks to join the cloud environment, then the cloud server redirected it to the (TPV) server to be scanned for any infection. After the (TPV) server scanned the node B for infection (malware).

The (TPV) server found that the target node is infected with some types of malwares. Then, the scanning result is sent to the cloud server to make the decision. And since the scanning result showed that the target node is infected, then the node request to join the cloud will be refused.

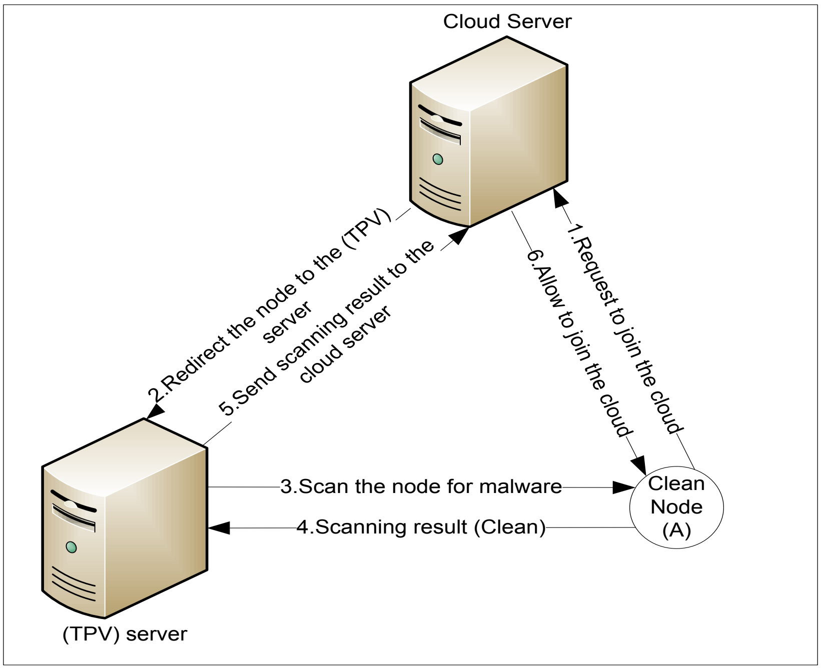
Cloud Server
2.Redirect the node to the (TPV) server
5.Send scanning result to the cloud server
6.Allow to join the cloud
1.Request to join the cloud
3.Scan the node for malware
4.Scanning result (Clean)
Clean Node (A)
(TPV) server

Fig. 3. Clean node asks to join the cloud environment

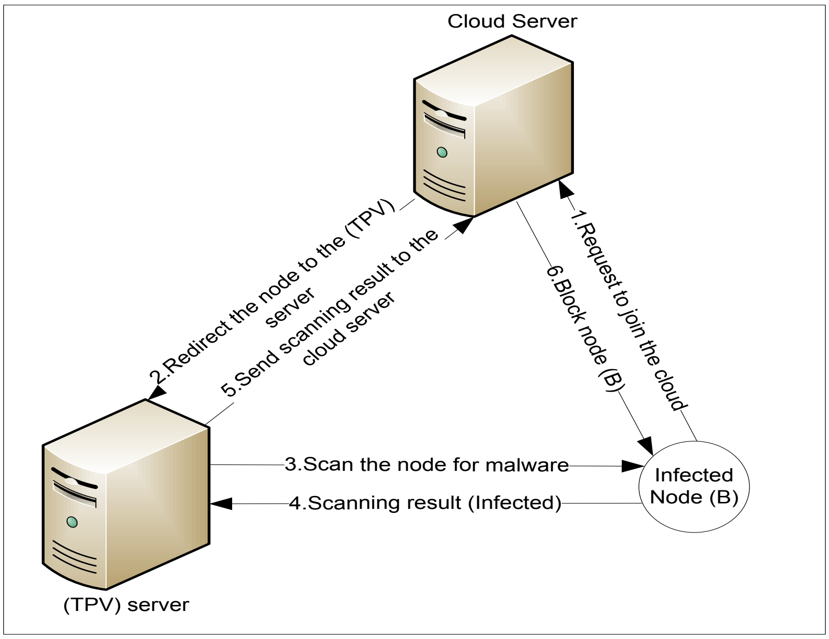
Cloud Server
2.Redirect the node to the (TPV) server
5.Send scanning result to the cloud server
6.Block node (B)
1.Request to join the cloud
3.Scan the node for malware
4.Scanning result (Infected)
Infected Node (B)
(TPV) server

Fig. 4. Infected node asks to join the cloud environment

6 Safety and Security Analysis:

An analysis of the proposed technique will be discussed in this section.
While the TPV server will scan the node when attempting to join the cloud, then:

- Only the clean nodes (not infected by malware) will be allowed to join the cloud environment.
- The cloud virtual machines as well as other clients' machines will be safe and protected from malware infection and threats

Definition 1 (Environment Security) The cloud environment is safe and secure from outsider as well as insider attacks and threats.

Theorem 1. The usage of TPV server makes the cloud environment secure against insider as well as outsider attacks and threats according Definition 1.

Proof. Here, we will prove that the cloud virtual machines as well as the existed nodes in cloud environment are secure against insider as well as outsider attacks and threats. As the TPV server scans the node which asks to join the cloud environment; only the clean nodes are allowed to join the environment. Consequently, the cloud environment will be safe and secure against insider as well as outsider attacks and threats.

7 Conclusion

The proposed technique makes it possible to distinguish between the nodes that run malicious softwares and attack tools from the clean ones. Which in turn reduces the risk of adding new nodes that may compose a threat to the cloud environment. Using the proposed technique, the decision making process of adding new node to the cloud environment became easier and proactively could eliminate the threats that may affect the cloud performance.

8 References

[1] Rajendran, P.K., B. Muthukumar, and G. Nagarajan, *Hybrid intrusion detection system for private cloud: a systematic approach.* Procedia Computer Science, 2015. **48**: p. 325-329. https://doi.org/10.1016/j.procs.2015.04.189

[2] Tandale, D.S. *Security on Cloud Computing*. in *International Journal of Engineering Research and Technology*. 2015. ESRSA Publications.

[3] Vaquero, L.M., L. Rodero-Merino, and D. Morán, *Locking the sky: a survey on IaaS cloud security*. Computing, 2011. **91**(1): p. 93-118. https://doi.org/10.1007/s00607-010-0140-x

[4] Jouad, M., et al. *Security challenges in intrusion detection*. in *Cloud Technologies and Applications (CloudTech), 2015 International Conference on*. 2015. IEEE.

[5] Fernandes, D.A., et al., *Security issues in cloud environments: a survey.* International Journal of Information Security, 2014. **13**(2): p. 113-170. https://doi.org/10.1007/s10207-013-0208-7

[6] Osanaiye, O.A. *Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing*. in *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*. 2015. IEEE.

[7] Patel, A., et al., *An intrusion detection and prevention system in cloud computing: A systematic review.* Journal of Network and Computer Applications, 2013. **36**(1): p. 25-41. https://doi.org/10.1016/j.jnca.2012.08.007

[8] Mazzariello, C., R. Bifulco, and R. Canonico. *Integrating a network ids into an open source cloud computing environment*. in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*. 2010. IEEE.

[9] Kannan, A., et al. *Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks*. in *Data Mining Workshops (ICDMW), 2012 IEEE 12th International Conference on*. 2012. IEEE.

[10] Egea, M., et al., *A certification framework for cloud security properties: the monitoring path*, in *Accountability and Security in the Cloud*. 2015, Springer. p. 63-77. https://doi.org/10.1007/978-3-319-17199-9_3

[11] Ab Rahman, N.H. and K.-K.R. Choo, *A survey of information security incident handling in the cloud.* Computers & Security, 2015. **49**: p. 45-69. https://doi.org/10.1016/j.cose.2014.11.006

[12] Bhadauria, R. and S. Sanyal, *Survey on security issues in cloud computing and associated mitigation techniques.* arXiv preprint arXiv:1204.0764, 2012.

[13] Gai, K., et al. *Proactive Attribute-based Secure Data Schema for Mobile Cloud in Financial Industry*. in *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*. 2015. IEEE.

[14] Yu, H., et al. *Cloud computing and security challenges*. in *Proceedings of the 50th Annual Southeast Regional Conference*. 2012. ACM. https://doi.org/10.1145/2184512.2184581

[15] Puthal, D., et al. *Cloud computing features, issues, and challenges: a big picture*. in *Computational Intelligence and Networks (CINE), 2015 International Conference on*. 2015. IEEE.

[16] Ali, M., S.U. Khan, and A.V. Vasilakos, *Security in cloud computing: Opportunities and challenges.* Information Sciences, 2015. **305**: p. 357-383. https://doi.org/10.1016/j.ins.2015.01.025

[17] Mell, P. and T. Grance, *The NIST definition of cloud computing.* 2011.

[18] Bakshi, A. and B. Yogesh. *Securing cloud from ddos attacks using intrusion detection system in virtual machine*. in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*. 2010. IEEE.

[19] Dastjerdi, A.V., K.A. Bakar, and S.G.H. Tabatabaei. *Distributed intrusion detection in clouds using mobile agents*. in *Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP'09. Third International Conference on*. 2009. IEEE.

[20] Shelke, M.P.K., M.S. Sontakke, and A. Gawande, *Intrusion detection system for cloud computing.* International Journal of Scientific & Technology Research, 2012. **1**(4): p. 67-71.

[21] Zarrabi, A. and A. Zarrabi, *Internet intrusion detection system service in a cloud.* 2012.

[22] Xin, W., H. Ting-lei, and L. Xiao-yu. *Research on the Intrusion detection mechanism based on cloud computing*. in *2010 International Conference on Intelligent Computing and Integrated Systems*. 2010.

9 Authors

Ashraf H. Aljammal (corresponding author) is with the Department of Computer Science and its Applications, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan (ashrafj@hu.edu.jo).

Hani Bani-Salameh is with the Department of Software Engineering, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan (hani@hu.edu.jo).

Ayoub Alsarhan is with the Department of Computer Information Systems, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan (ayoubm@hu.edu.jo).

Mohammad Kharabsheh is with the Department of Computer Information Systems, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan (mohkh86@hu.edu.jo).

Mamoon Obiedat is with the Department of Computer Information Systems, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan (mamoon@hu.edu.jo).

Article submitted 08 December 2016. Published as resubmitted by the authors 13 February 2017.