An Immuno-based Autonomic Computing System for IaaS Security in Public Clouds

Abdelwahhab Satta, Sihem Mostefai and Imane Boussebough
Department of Fundamental Computer Science and Applications, University of Constantine 2, Constantine, Algeria

Keywords: Cloud Computing, IaaS, Autonomic Computing Systems, Artificial Immune Systems.

Abstract: Cloud Computing is the new way for computing infrastructures exploitation. These infrastructures, offered as a service by the cloud IaaS service model are being very appealing to the new industry and business. However, surveys reveal that security issues are still the major barrier facing the migration from Infrastructure in premise to public clouds. On the other hand, Autonomic Computing Systems have been used so far to enable the cloud, and in this work, we will investigate these systems capabilities to enable security management for IaaS in public clouds.

1 INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services, etc.) (Mell and Grance, 2011). Services offered by the cloud computing are categorized in service models as described by the SPI framework where the letters stand for 'Software', 'Platform' and 'Infrastructure' (Hill et al., 2012).

Despite the benefits of cloud computing adoption, there are also some significant barriers; two of the most relevant are security and privacy (Mather et al., 2009).

In the last few years, emergent bio-inspired complex systems defined as Autonomic Computing Systems (Kephart and Chess, 2003) have gained more importance and attention in computer science community due to their efficiency and performance.

In this work, we will investigate major security issues in IaaS service model in public clouds and the different sources and levels of these issues; then we will propose a security system based on Autonomic Computing Systems principles and Artificial Immune Systems models to mitigate these issues.

This paper is organized as follows. Section 2 presents a state of the art on the IaaS service model and security issues related to its adoption in public clouds. We will also present the Autonomic Computing Systems (ACSs), the Artificial Immune Systems (AISs), and their contributions to computer security. Section 3 presents related works regarding IaaS security issues in public clouds and introduces recent interests for Autonomic Computing cyber defence systems. Then section 4 presents the proposed system architecture and the underlying components details. Finally, section 5 presents the conclusion and the prospects of this work.

2 BACKGROUND

2.1 Cloud Infrastructure as a Service

According to the National Institute of Standards and Technology (NIST), IaaS is the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls) (Mell and Grance, 2011).

IaaS is the lowest layer in the SPI framework stack and arguably the most established cloud service model already offering a wide variety of products and advanced capabilities such as automated scalability, pay-per-use, and on-demand infrastructure provisioning (Vaquero et al., 2011).

Satta, A., Mostefai, S. and Boussebough, I.
An Immuno-based Autonomic Computing System for IaaS Security in Public Clouds.
DOI: 10.5220/0006352405740581
In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 546-553
ISBN: 978-989-758-243-1

Developers still have to design and code entire applications and administrators still need to install, manage, and patch third-party solutions, but there is no physical infrastructure to manage anymore (Kavis, 2014).

IaaS could be the preference of many businesses, according to their requirements for performance, scalability, downtime mitigation and recovery from a vendor outage, more than gaining control of their infrastructure (Vaquero et al., 2011).

2.1.1 Security Issues in IaaS in Public Cloud Business Model

When discussing security issues in IaaS, it is mandatory to reveal the impact of the public business model. Cloud computing infrastructure security is greatly affected by whether the employed cloud is private or public.

With private or internal clouds, there are no new attacks, vulnerabilities or changes in risk that information security personnel need to consider, and security considerations of traditional IT remain applicable. However, if consumers choose to use public cloud services, changing security requirements will require changes to their network topology. They must address how their existing network topology interacts with their cloud provider's network topology (Mather et al., 2009).

NIST defines a public cloud as a cloud infrastructure that is made available to the general public or a large industry group and that is owned by an organization selling cloud services (Mell and Grance, 2011). This resource sharing of not only physical machines but also networks enables maximum utilisation of the available assets, at the cost of introducing delicate multi-tenancy concerns (Vaquero et al., 2011).

Multi-tenancy concerns are mainly raised by the virtualization that is a key enabling technology for the cloud. The transformation from dedicated to shared infrastructure embodies a series of threats and vulnerabilities. Data leakage by exploiting VMs or hypervisor vulnerabilities is the main virtualization risk (Gonzales et al., 2015; Vaquero et al., 2011).

Moreover, cloud computing requires universal access and connectivity to the Internet to thrive (Krutz and Vines, 2010). This costs public clouds other rigorous security concerns inherited from Internet technologies and even if an enormous amount of security is put in place in the cloud, still the data is transmitted through the normal underlying Internet technology. Therefore, the security concerns threatening the Internet are also threatening the cloud (Subashini and Kavitha, 2011).

Another dimension of IaaS security issues is essentially related to the cloud consumers' nature. Start-ups and Small to Medium-size Businesses (SMBs) are major cloud services consumers. These enterprises usually do not have large IT departments and do not govern security management in public clouds.

IaaS vendors provide the entire infrastructures to the consumers to run their applications, and since these consumers are given full access to this virtual infrastructure, they are responsible for ensuring their proper security and ongoing security management (Mather et al., 2009). This could be extremely problematic for SMBs embracing IaaS.

2.1.2 Infrastructure Security

Non-information security professionals are cautioned not to simply equate infrastructure security to IaaS security. Securing an organization's core IT infrastructure at the network, host and application levels is a commonly used approach by information security practitioners. Then, the infrastructure security can be viewed, assessed and implemented according to each one of these levels (Mather et al., 2009).

A. Network Level

If public cloud services were chosen, four significant risk factors should be addressed (Mather et al., 2009):

- Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider;
- Ensuring proper access control to whatever resources that are used at the public cloud provider;
- Ensuring the availability of the Internet-facing resources in a public cloud that are being used by an organization, or have been assigned to an organization by public cloud providers;
- Replacing the established model of network zones and tiers with domains.

B. Host Level

Host security in IaaS should be categorised as follows (Mather et al., 2009):

- Virtualization software security;
- Customer guest OS or virtual server security. IaaS customers have full access to virtualized guest VMs, they also take full responsibility of their ongoing security management.

C. Application Level

Application or software security is the third level of infrastructure security and should be a critical

element of any security program. IaaS customers have full responsibility for securing their applications. This level of infrastructure security must address (Mather et al., 2009):

- Web applications security threats;
- End user security;
- Public cloud security limitations.

In summary, infrastructures security challenges are not specifically caused but instead are exacerbated by cloud computing. IaaS customers have full control over their provisioned assets; hence, they take full responsibility to ensure their security management (Mather et al., 2009).

2.2 Autonomic Computing

IBM, in (Kephart and Chess, 2003) states that the need to integrate several heterogeneous environments into corporate-wide computing systems and to extend that beyond company boundaries, goes well beyond the administration of individual software environments, more than it introduces new levels of complexity. As computing evolves, the overlapping connections, dependencies, and interacting applications call for administrative decision-making and responses faster than any human can deliver.

The growing complexity of the IT infrastructure threatens to undermine the very benefits information technology aims to provide. Therefore, dealing with this complexity is the single most important challenge facing the IT industry (Horn, 2001).

The term Autonomic Computing was first used by IBM in 2001 to describe computing systems that are said to be self-managing. However, the concepts behind self-management were not entirely new to IBM's autonomic computing initiative (Huebscher and McCann, 2008).

Autonomic Computing Systems are systems capable of running themselves, adjusting to varying circumstances, and preparing their resources to handle most efficiently the workloads we put upon them (Horn, 2001).

The main properties of self-management as portrayed by IBM are self-Configuration, self-Optimization, self-Healing, and self-Protection, or Self-CHOP properties as widely called (Huebscher and McCann, 2008). These properties could be defined as follows (Kephart and Chess, 2003):

Self-configuration: Automated configuration of components and systems following high-level policies. The rest of the system adjusts automatically and seamlessly.

Self-optimisation: Components and systems continually seek opportunities to improve their own performance and efficiency.

Self-healing: The system automatically detects, diagnoses and repairs localised software and hardware problems.

Self-protection: The System automatically defends against malicious attacks or cascading failures. It uses early warning to anticipate and prevent system-wide failures.

2.3 Artificial Immune Systems

The natural immune system is a complex biological and an autonomic system with a highly distributed, robust, adaptive and self-organizing nature for self-protection (Dasgupta, 2007). This system is able to categorize all cells or molecules within the body as self or non-self and to defend the body against foreign pathogens. It achieves this with the help of a distributed task force that has the intelligence to take action from a local and also global perspective using its network of chemical messengers for communication (Aickelin et al., 2014).

Artificial Immunes Systems are a novel emerging computational intelligence technique inspired by immunology. These systems invest in the powerful information processing capabilities of natural immune systems such as feature extraction, pattern recognition, learning, memory, multi-layered protection, diversity and distributive nature that provide the ability to perform many complex computations in a highly parallel and distributed fashion (Dasgupta, 1993).

From the information processing point of view, immunological principles are very important in developing next generation cyber defence systems (Dasgupta, 2007).

The following mechanisms and theories are primarily used in AISs models (Dasgupta and Gonzalez, 2003):

Immune Network Theory: It has been proposed in the mid-seventies. Where the immune system maintains an idiotypic network of interconnected immune cells.

Negative Selection Mechanism: The purpose of negative selection is to provide the discrimination between self and nonself cells. It deals with the immune system's ability to detect unknown antigens while not reacting to the self-cells.

Clonal Selection: The clonal selection principle describes the basic features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigen proliferate, thus being selected against those that do not.

Danger Theory: The central idea in the Danger

Theory is that the immune system does not respond to non-self but to danger (Cayzer and Aickelin, 2002). The danger theory (DT) model appears to be more appropriate in the cyber world as not all abnormal events represent attacks (Dasgupta, 2007).

3 RELATED WORKS

Cloud IaaS security is becoming a very large discussion topic in the last few years. In (Vaquero et al., 2011) the authors survey the most relevant threats for the cloud and focus on security issues in IaaS in public cloud deployment. In addition, they illustrate where the dangerous points lurk at every level in a typical IaaS cloud architecture. Those issues have been also surveyed in (Huang et al., 2015); where the authors identify security problems and solutions described in academia. Furthermore, they focus on industry best practices and compare them with the academia research contributions.

In general, most of the works presented by these surveys and others could be included within the previous infrastructure security three level model.

In the network level, most of the works rely on Network Overlays (Vaquero et al., 2011), firewall rules, VLAN traffic segregation and Software Defined Networks (SNDs) (Yeluri and Castro, 2014), (Ahmad et al., 2015). They also rely on Intrusion Detection and Prevention Systems (IDSs, IPSs), IDS/IPS combination, cryptographic protection and VPNs to connect to a remote cloud or to a publicly hosted cloud provider (Modi et al., 2013), (Xing et al., 2013).

In the host level, for hypervisor and guest OS security, boot integrity checking and attestation, isolation of hypervisor management traffic from applications traffic (Yeluri and Castro, 2014), Side-Channel attack detection and mitigation systems (Zhang et al.,2016), Homomorphic Encryption (Liu, 2014), VM image templating and management systems (Vaquero et al., 2011), (Kavis, 2014), account restriction and enhanced authentication techniques, Lightweight directory access protocol (LDAP) and Single Sign-On (SSO) based mechanisms (Zissis and Lekkas, 2012), instance-level firewalls, host-based variants of IDS and IPS (HIDS/HIPS), antiviruses, patch and configuration management systems, and logging are the most relevant to mention (Mather et al., 2009), (Hill et al., 2012), (Modi et al., 2013).

At last, in the application level, several works propose to include security in the software development life cycle (SDLC) (Mather et al., 2009), application auditing, patch management, accounts restriction, etc. (Hill et al., 2012).

In summary, employment of current IDS approaches lacks the proactive capability to prevent attacks at its initial stage. Moreover, it requires hiring expensive professional security experts. On the other hand, IPS approaches are employed in order to automatically take action towards any suspect event. However, there are several issues in the current IPS systems such as *latency*, *accuracy*, and *flexibility* that make their use not appropriate for some delay-sensitive services (Xing et al., 2013).

This raises the need for automated threat response systems capable of ensuring efficient, reliable, flexible and seamless security management for overwhelming issues in the cloud, such as ACSs.

Many works that are inspired by natural Autonomic Systems such as (Harmer et al., 2002), (Dasgupta, 2007), (Rufus et al., 2016) arose in this field in the last few years. However, almost all of them are for general cyber defence and not adapted to the cloud-specific features.

4 PROPOSED APPROACH

In this work, we aim to design an Autonomic Computing defence system that has the capability of responding to security incidents in the operating environment which is the public cloud infrastructure provisioned by a consumer of IaaS. The system's architecture is independent and is not coupled with the underlying virtual or physical cloud infrastructure. Therefore, it makes the system capable of being integrated within any customer infrastructure for maintaining an automated, proactive, highly distributed and seamless security management in each level of the infrastructure.

This approach comes from the principle that the concept of security for the cloud services does not so much rely on new technology, but is more a rethink in terms of how existing solutions are deployed (Hill et al., 2012).

4.1 Proposed Architecture

Our architecture is based on industry best practices and adapted to the dynamic nature of an elastic infrastructure. Separate storing of logging information from the physical servers where the logs are created so that the information is not lost when the cloud resources go away is a common approach in cloud industry (Kavis, 2014). These logs would feed an artificial immune system by instant and valuable

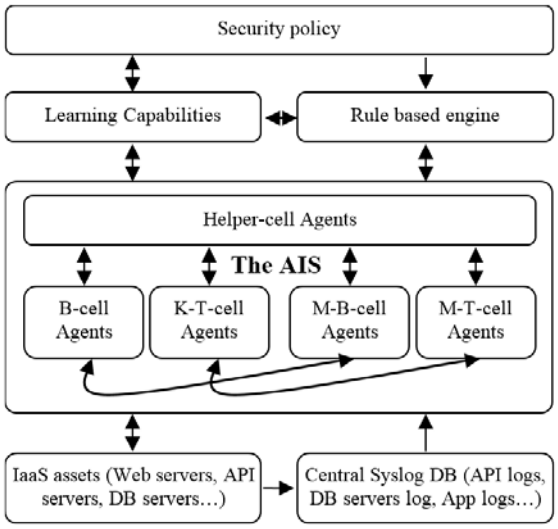

Figure 1: The overall architecture of the system.

information about the behaviour and the security state of the elastic consumer-provisioned assets. This approach makes the response of the security system instant and effective. Figure.1 presents the overall architecture of the system and the underlying components.

The AIS is the most crucial component in this architecture. It is responsible with the rule-based engine and the security policy repository of presenting an immune response behaviour against any internal or external security threat in the provisioned assets. The immunological principles of the AIS (self-nonself discrimination, negative selection, danger theory, etc.) provide for this architecture the diversity and the highly distributed control and processing necessary to enable the emergent defence behaviour.

Moreover, this architecture provides the system with learning capacities based on the feedback from the AIS in order to ensure the system's continued evolution and maturation over time.

4.1.1 System Components Description

The emerged defence behaviour of this security system is the result of the cooperation of its underlying components.

A. AIS Component

The AIS in this architecture plays both the roles of proactive detection and response to any internal or external security threat. This AIS receives its entries from the operating environment and are basically the logged events from the customer's current assets. At this point, this system relies on the self-non-self discrimination and the danger theory to determine whether the logged event represents an abnormal behaviour and whether this abnormal behaviour is a security danger.

As its natural counterpart, this system is composed of several immune cell types that are represented as agents:

The *helper-cell* agents are analogous to natural *Macrophage* and *Helper-T cells* and have two main tasks:

Firstly, these agents employ proactive monitoring, and Data mining on the logging base to inspect all the levels of the infrastructure such as network traffic, VMs resources usage, servers activity, users access, applications warnings, errors, and other information, and compare them with a defined normal behaviour to perceive any abnormal behaviours at the instant they occur. The correlation of gathered information significantly increases the system's accuracy and diminishes false alarms problem in current IDSs. Moreover, this technique enhances the system's diversity and reliability since implementing intrusion detection becomes simpler on top of a central logging database (Kavis, 2014).

In addition, these *helper-cell* agents are also responsible for systematic vulnerability assessment procedures of the provisioned assets as another resource of security information.

Secondly, In the case of perceiving danger, the *helper-cell* agents are responsible for stimulation, proliferation, and differentiation of *B-cell* and *Killer-T-cell* (*K-T-cell*) agents.

The *B-cell* and *K-T-cell* agents operate on the provisioned assets and provide the system with an adaptive immune response. Activated *B-cell* agents are responsible for destroying invaders or antigens that could be for example malicious traffics, malicious injected VMs, viruses, worms, or any identified nonself in each level of the infrastructure.

Another type of immune response is also provided with *K-T-cell* agents and is oriented against altered-self components of the infrastructure; these components could be altered configurations, compromised VMs, malicious insiders, etc.

In the activation step, a *B-cell* or a *K-T-cell* agent receives from a *helper-cell* agent an activation signal that contains the invaders or the altered-selves features and the corresponding countermeasures propagated from the rule-based engine.

The *M-B-cell* and *M-T-cell* agents are differentiated clones of an activated *B-cell* or *K-T-cell* agent respectively. These agents live longer and memorise information about the encountered threat and the corresponding applied countermeasures for

any future similar case to allow an response, and reduce non-necessary performance consuming interactions.

B. Learning Capabilities Component

Based on the feedback from the AIS system, this component functioning is also autonomous and is responsible for maintaining continuous evolution and maturation of the overall system over time, including the security policy and the rules of the rule-based engine. Encountered threats, applied countermeasures, and costs of the immune response would be entries to learning engines within this module.

C. Security Policy Repository and Rule Based Engine Components

Procedural programming is well suited for problems in which the inputs are well specified and for which a known set of steps can be carried out to solve the problem (Friedman-Hill, E., 2003).

Therefore, a procedural approach is not appropriate in this case, and we adopt a declarative Rule-based system approach using a rule-based engine and a policy repository to deploy the security policy. Moreover, this approach also supports the feasibility and simplify the implementation of the system.

4.1.2 System Components Interactions

A scenario of the events and interactions between the system's components in response to a first time encountered security issue is depicted in Figure 2.

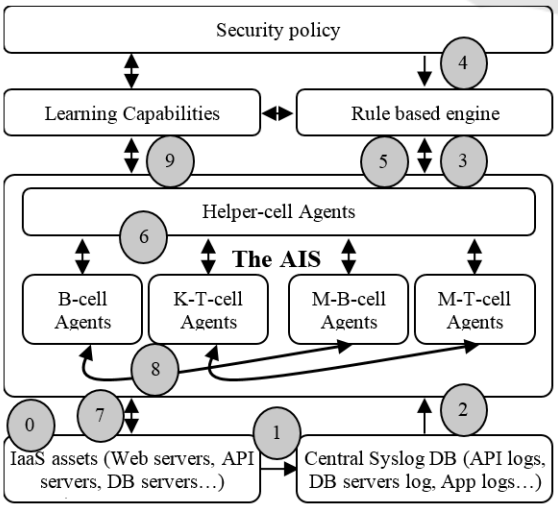

Figure 2: Example of messages exchanged between the systems' components in a first response to a security issue scenario.

0. An unforeseen security issue occurs.
1. The security issue is logged to the logging database
2. A *helper-cell* agent retrieves and analyses the logged events entries at the instant they occur.
3. The *helper-cell* agent senses a danger and asks the corresponding countermeasures from the rule-based engine because the perceived danger is a first time encountered.
4. The rule-based engine carries the adequate policy rules to apply from the security policy base.
5. The *helper-cell* agent receives the corresponding countermeasures for the perceived issue from the rule-based engine.
6. The *helper-cell* agent sends an activation signal that contains the identified danger features and the corresponding countermeasures to a *B-cell* or *K-T-cell* agent according to the danger source origin.
7. The activated agent proliferates and proceeds to eliminate the issue.
8. The activated agent differentiates to create memory clones.
9. The AIS agents send the feedback information to the learning capabilities component.

4.2 Self-CHOP Properties of the System

When the system is integrated for the first time to its operating environment, or if determined necessary when the infrastructure scales up or down, a *self-configuration* process of the system is mandatory in order to maintain a coherent configuration of its underlying components with the current infrastructure state.

Triggered by the detection of any abnormal behaviour, security recovering procedures or *self-healing* processes are applied for repairing compromised software or hardware components in the provisioned assets.

A *Self-optimisation* process based on the feedback control and the embedded learning mechanisms besides the native ones of the AIS provide continuous improvement and maturation for the system's efficiency and performance over time.

At last, *self-protection* property of an ACS. Maintaining overall environment security and integrity against malicious internal or external attacks invasions is the major purpose of this architecture and is achieved by the synergetic behaviour resulting from the system's components cooperation.

5 CONCLUSION AND PROSPECTS

In this work, we have presented an Autonomic Computing security system based on an Artificial Immune System model and a Rule-based System architecture. We have discussed how this system provides the necessary flexibility to handle the dynamic nature of an elastic cloud infrastructure and the necessary robustness to ensure a security healthy state for the public IaaS infrastructures. We have also discussed how this system's architecture encourages the self-CHOP properties and invests in the characteristics of the AISs.

We are currently working on selective strategies and methods to be used within the AIS. These methods would conduct the infrastructure state monitoring and control the security danger definition and sensation, the activation and the proliferation of the immune cells agents, and mechanisms to provide the learning capabilities for the overall system.

In future works, we will be presenting a more detailed architecture of this system through these selective strategies and methods and a realisation of the ACS self-CHOP properties. We will also be presenting a straightforward implementation details and experimental results of this system's prototype deployment on real IaaS environments such as AWS or RackSpace infrastructures.

REFERENCES

Ahmad, I., Namal, S., Ylianttila, M. and Gurtov, A., 2015. Security in software defined networks: A survey. IEEE Communications Surveys & Tutorials, 17(4), pp.2317-2346.

Aickelin, U., Dasgupta, D. and Gu, F., 2014. Artificial immune systems. In Search Methodologies (pp. 187-211). Springer US.

Cayzer, U.A.S., 2002. The danger theory and its application to artificial immune system. In Proceedings of the 1st International Conference on Artificial Immune Systems (pp. 141-148).

Dasgupta, D., 1993. An overview of artificial immune systems and their applications. In Artificial immune systems and their applications (pp. 3-21). Springer Berlin Heidelberg.

Dasgupta, D., 2007. An immuno-inspired autonomic system for cyber defense. Information security technical report, 12(4), pp.235-241.

Dasgupta, D., Ji, Z. and Gonzalez, F., 2003, December. Artificial immune system (AIS) research in the last five years. In Evolutionary Computation, 2003. CEC'03. The 2003 Congress on (Vol. 1, pp. 123-130). IEEE.

Friedman-Hill, E., 2003. JESS in Action (Vol. 46). Greenwich, CT: Manning.

Gonzales, D., Kaplan, J., Saltzman, E., Winkelman, Z. and Woods, D., 2015. Cloud-trust-a security assessment model for infrastructure as a service (IaaS) clouds. IEEE Transactions on Cloud Computing.

Harmer, P.K., Williams, P.D., Gunsch, G.H. and Lamont, G.B., 2002. An artificial immune system architecture for computer security applications. *IEEE transactions on evolutionary computation*, *6*(3), pp.252-280.

Hill, R., Hirsch, L., Lake, P. and Moshiri, S., 2012. Guide to cloud computing: principles and practice. Springer Science & Business Media.

Horn, P., 2001. Autonomic computing: IBM\'s Perspective on the State of Information Technology.

Huang, W., Ganjali, A., Kim, B.H., Oh, S. and Lie, D., 2015. The state of public infrastructure-as-a-service cloud security. ACM Computing Surveys (CSUR), 47(4), p.68.

Huebscher, M.C. and McCann, J.A., 2008. A survey of autonomic computing—degrees, models, and applications. ACM Computing Surveys (CSUR), 40(3), p.7.

Kavis, M.J., 2014. Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, AND IaaS). John Wiley & Sons.

Kephart, J.O. and Chess, D.M., 2003. The vision of autonomic computing. Computer, 36(1), pp.41-50.

Krutz, R.L. and Vines, R.D., 2010. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

Liu, D., 2014. Securing Outsourced Databases in the Cloud. In Security, Privacy and Trust in Cloud Systems (pp. 259-282). Springer Berlin Heidelberg.

Mather, T., Kumaraswamy, S. and Latif, S., Cloud Security and Privacy (2009).

Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in the cloud. Journal of Network and Computer Applications, 36(1), pp.42-57.

Rufus, R., Nick, W., Shelton, J. and Esterline, A., 2016. An Autonomic Computing System based on a Rule-based Policy Engine and Artificial Immune Systems.

Subashini, S. and Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), pp.1-11.

Vaquero, L.M., Rodero-Merino, L. and Morán, D., 2011. Locking the sky: a survey on IaaS cloud security. Computing, 91(1), pp.93-118.

Xing, T., Huang, D., Xu, L., Chung, C.J. and Khatkar, P., 2013, March. Snortflow: A openflow-based intrusion prevention system in cloud environment. In Research and Educational Experiment Workshop (GREE), 2013 Second GENI (pp. 89-92). IEEE.

Yeluri, R. and Castro-Leon, E., 2014. Building the Infrastructure for Cloud Security: A Solutions View. Apress.

Zhang, T., Zhang, Y. and Lee, R.B., 2016, September. Cloudradar: A real-time side-channel attack detection system in clouds. In International Symposium on Research in Attacks, Intrusions, and Defenses (pp. 118-140). Springer International Publishing.

Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), pp.583-592.