*This is a Pre-Print Version of the paper. The final paper was published in Proceedings of* "The 2nd International Conference on Applied Information and Communications Technology" - ICAICT 2014

ISBN: xxxxxxxxxxxx

# Securing the Cloud against Distributed Denial of Service Attacks: A Review

Mohammed M. Alani*

*Middle East College, KOM, Muscat 124, Oman*

**Abstracts**

Distributed denial of service attacks are becoming a serious threat that no business involved in providing services over the Internet can ignore. The rapidly growing frequency and magnitude in which these attacks are occurring is an alarming indicator. As cloud services are being adopted by many enterprises, the cloud infrastructure resilience to such attacks becomes a growing concern. In this paper, we discuss the types and possible impacts of DDoS attacks on cloud computing and the suggested mitigation techniques. These attacks were categorized into three categories; external, internal, and cloud-to-outside attacks.

*Keywords:*cloud; security; denial of service; dos

## 1. Introduction

With rapidly increasing applications on the Internet, people rely more and more on Internet-based services in their regular daily actions. Availability of these services have grown to be one of the biggest concerns for both clients and service providers. During the past few years, many attacks have targeted availability of Internet-based services.

Denial of Service (DoS) attacks aim at making a certain network service unavailable to its legitimate users. In its basic form, this attacks keep the resources busy such that these resources become unavailable to the users this service was aimed to serve. [1]

As network security research grew stronger, simple DoS attacks were less effective and easily detectable. Since the regular DoS attack comes from a single source, it becomes less effective once the source is detected by security appliances, or software, and blocked. A more sophisticated and harder to detect version evolved, namely Distributed Denial of Service (DDoS) attack.

In DDoS attack, a DoS attack is launched from multiple sources, usually tens or hundreds, at the same time. Because it is coming from multiple source, DDoS attack is harder to detect and deter as compared to simple DoS attacks.

* Corresponding author. Tel.: +968-24531488; fax: +968-24446028.
*E-mail address:* m@alani.me

Reports show that only six DDoS attacks took place in the year 1988. The year 2000 witnessed DDoS attacks on large websites like CNN, Yahoo, and Amazon. At that time, reports shown that DDoS attack rates reached 1GBps. In 2007, DDoS attacks reached the rates of 70GBps. In 2013, a huge attack took place on Spamhaus spam detection service that reached the huge rate of 300 GBps [1]. In February 2014, the largest DDoS attack in history took place with the rate of 400 GBps which is the largest known DDoS attack known until now [2]. The largest DDoS attack in history mentioned earlier targeted a public cloud service provider called CloudFlare. Attacks of such magnitude affect not only their targets, but affect the overall Internet in the area. As mentioned in [2], regular Internet users experienced noticeable slowness in their Internet services.

The dynamic nature of cloud computing can be beneficial to counter DDoS attacks in some scenarios. However, the different levels at which DDoS attacks can be performed on a cloud-based service can make defence more complex, as we will see in the next sections.

## 2. Anatomy of a DDoS Attack

The open nature of the Internet makes it hard to identify attackers involved in a DDoS. In general, DDoS can be performed in two methods. The first is done through sending a one or more carefully crafted packets to the target that can cause the target computer to halt or reboot, like the Ping-of-Death attack [3]. This method relies on vulnerabilities in the operating system or other parts of the system and exploits these vulnerabilities to render the system unusable. This method can be countered by updating and patching the system in regular manner. The second method, which is the most common one, tries to exhaust the resources of the target by flooding it with huge amounts of traffic. This huge amount of traffic consumes different resources until one, or more, of them is fully exhausted that renders the system unavailable. The targeted resources can be bandwidth, memory, processing power, or even battery power in systems with limited power supply like mobile devices. Figure 1 shows how DDoS attacks are carried out by an attacker.

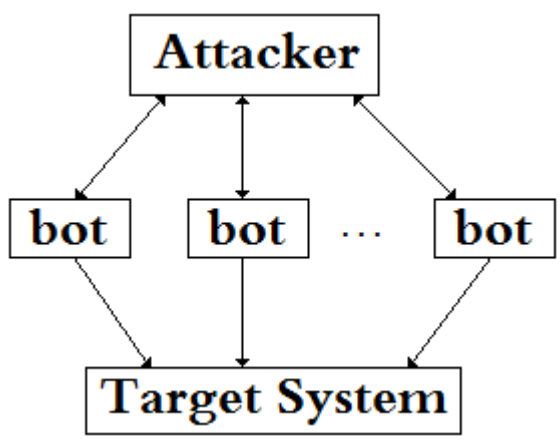


Fig 1 How DDoS Attacks are Performed

As DDoS attack involves more than a single host acting as a source of the attack, in most cases, attackers use computers or servers of other users who are unaware that their devices are being employed in an attack. It would be difficult for a huge group of attackers to attack from their own computers only because the number of attacking devices would be limited and might be traceable. Thus, attackers penetrate other computers and/or servers and inject them with attacking bots, short of Internet Robots. In general, bots are small software applications that run automated operations on a remote computer over the Internet based on pre-configured sequence or on commands

received from the bot creator. The attacker implants these bots in the computers/servers that will later be used in the attack and makes sure that the operation of the said computers/servers is not disturbed. This way, the unknowing users of these computers/servers will not detect the penetration that happened and thus prevent the attack from being launched from their systems.

## 3. Cloud Architecture and Service Models

A cloud computing system can be divided into logical layers to simplify its architecture, as shown in Fig.2. At the bottom, the hardware layer exists. This layer contains the storage components, memory, and processors. Above the hardware layer, abstraction layer software exists. This abstraction layer software is aware of the identifying characteristics of cloud computing and it is the layer responsible for controlling the provision of services to clients. This layer is often called the hypervisor. Above this layer of abstraction lie three layers Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Each one of these layers represent a service model of cloud computing.

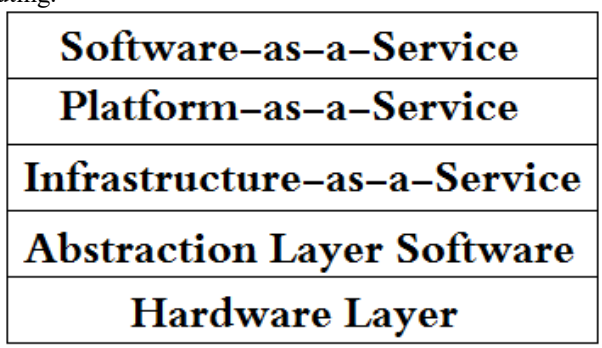


Fig 2 Cloud Computing Layers

Before proceeding into the details of cloud service models, two more identifications need to be made; public and private clouds. A *public cloud* is the cloud service managed and provided to client, usually with a certain fee, by an organization to the general public. Examples of public clouds are Amazon E2C and Microsoft Azure. This type of clouds provides services to multiple clients. A *private cloud* is a cloud service owned, provided, and managed by an organization for the private use of the organization itself. This type of cloud provides services only to this particular organization. In certain occasions, a *hybrid cloud* can be partially public, and partially private

### *3.1. Infrastructure-as-a-Service*

IaaS service model is the lowest level of service provided to the client. In this service model, the cloud computing client is provided with controlled access to the virtual infrastructure. Using this access, the client can install operating system and application software. From the client's point of view, this model is similar to renting the hardware from a service provider and letting the service provider manage the hardware. In this sense, the client does not have control over the physical hardware. On the other hand, the client will have to manage the security aspects from the operating system and up to the applications. This model requires the client to have highly experienced network engineer(s). Handling everything from the operating system and up is a big responsibility that most clients decline to handle, especially because of the security burdens. Thus, this model is not of high preference in the cloud computing clients' society [4].

 

### *3.2. Platform-as-a-Service*

In PaaS, the operating system and all platform-related tools (like compilers) are already installed for the client. These pre-installed components are also managed by the cloud service provider.

Clients have the freedom of installing additional tools based on their needs. However, the control over the infrastructure is retained by the service provider. The client controls applications development, configuration, and deployment. In some aspects, this service model is similar to the traditional web-hosting services in which clients rent a remote server with development platform pre-installed on it. The major difference between this model and traditional web-hosting is the rapid provisioning. Traditional web-hosting is managed manually and requires human intervention when the demand increases or decreases. On the other hand, provisioning in cloud computing is automatic and rapid. Thus, it does not require any human interventions [4].

### *3.3. Software-as-a-Service*

SaaS model focuses on the application level and abstracts the user away from infrastructure and platform details. Usually, applications are provisioned via thin client interfaces such as web browsers or even mobile phone apps [4].

Microsoft's Outlook.com is a clear example of this. An organization can adopt Outlook.com electronic mail service and never bother with hardware maintenance, service uptime, security, or even operating system management. The client is given the control over certain parameters in the software configuration, for example, creating and deleting mail boxes. These parameters can be controlled through the interface of the application.

## 4. DDoS and the Cloud

In addition to targeting service availability, DDoS attacks have another harmful side in cloud computing. Almost all cloud service providers charge their clients based on the resources they consume. When a client is under DDoS attack, the attack consumes huge resource such that the financial implications caused can be devastating to the client organization.

When one client is using a public cloud service, the cloud infrastructure is shared with other clients. If a DDoS attack is carried out on one client, the attack can bring down the whole cloud and other clients will suffer from service disruption or complete unavailability.

In most cases, being at the receiving end of a DDoS attack is analogous to being caught in traffic jam; there is nothing that you can do to get to your destination neither can you turn back. All you can do is waiting. The service outage becomes very frustrating to clients and they start re-considering the reasons why they moved their data to the cloud [5].

DDoS attacks in cloud computing can occur on any one of the layers explained in the previous section starting from the lowest level of hardware. The attacker can try to flood the cloud with requests in such a rate that consumes all the bandwidth at the border of the cloud and make the service unavailable. In most cases, attackers perform more complex attacks at higher levels trying to exploit certain weaknesses in the system.

In order to better understand the nature of attacks and their mitigation techniques, we will categories the attacks into three categories; internal attacks, external attacks, and cloud-to-outside attacks. Internal attacks are attacks launched from within the cloud to target another instance in the same cloud. External attacks are attacks launched from outside the cloud to target a virtual machine or more in the cloud. Cloud-to-outside attacks are attacks launched from within the cloud targeting host(s) outside the cloud.

### *4.1. Internal Attacks*

Many types of attacks in cloud computing, including DoS, can cause more harm if conducted from within the cloud. The key into this type of attacks is co-residency detection. Co-residency detection through virtualization side channel was first introduced in [6]. After co-residency detection, the attacker can use a co-existing cloud instance to attack neighbor virtual machines hosted in the same physical machine. Another method of detecting co-residency was introduced in [7]. This method, named co-resident watermarking, relies on active traffic analysis and injects a watermark signature into the network flow of the target virtual machine. In [8], Game Theory defense mechanisms were employed to detect DoS attacks launched from co-resident instances. This new method has proved success in detecting DoS attacks. The proposed system relies on modeling the attack as a two-player game and recommends strategies of defending against similar attacks.

### *4.2. External Attacks*

Due to the billing model of cloud computing, new type of attacks, basically derived from DDoS attack has evolved; Fraudulent Resource Consumption (FRC) attacks. FRC attacks aim at launching an attacks similar to DDoS but in low intensity. This attack does not aim at making the service unavailable. It aims at overusing the service in such a way that the resulting financial implications on the cloud service client become very high. A method of detecting such attacks was described in [9]. In this study, three different attack scenarios were experimented. The experiments has shown that an attacker without knowledge of the web log has a difficult time mimicking the self-similar and consistent request semantics of normal web activity.

The impact of DoS and DDoS attacks on virtual machines can be severe if no quick action is taken to detect and deter these attacks. In [10], an initial study of virtual machines performance when they go under a DoS attack was introduced. This study has shown that even with relatively light DoS attacks, memory access and file system performance degrades severely as compared to non-virtualized systems under the same attack. The study also introduced a modified package of Linux KVM VirtIO drivers that is aimed to reduce the performance impact of DoS attacks by up to 40%.

Experiments were done on a quantitative solution to detect DoS and DDoS in [11]. These experiments were conducted in a private cloud architecture using Eucalyptus open-source cloud. This detection system proposed in this paper was a VM-based intrusion detection system. The suggested method has proven 65% detection rate with 2.6% false-positive. This success rate was for attacks conducted were ICMP-flooding, UDP-flooding, and TCP SYN-flood attacks.

Another paper suggesting a model to prevent flooding attacks in the cloud was presented in [12]. The proposed model, named Flooding Attack Prevention Architecture (FAPA), focused on allowing dynamic response that is capable of adapting any type of flooding attack.

In [13], a framework was proposed to detect and prevent DoS attacks and other malicious activities at the network layer. The framework suggested in this paper integrates a Network Intrusion Detection System (NIDS) within the cloud infrastructure. The framework also employs Snort intrusion detection system and decision tree classifier. Attacks are detected by monitoring network traffic while maintaining acceptable performance. The suggested framework was tested with the freely available NSL-KDD and KDD experimental intrusion datasets and the results showed 96% accuracy for KDD and 84% for NSL-KDD datasets.

An important concept was introduced in [14]. This paper suggested the creation of virtual machine that ran Snort intrusion detection system between the VMware hypervisor and all guest virtual machines connected to a virtual switch. This IDS system was capable of detecting DDoS attacks and then blocking the attackers by Snort. Afterwards, the VM was automatically moved to a new location in the cloud. Despite the fact that the paper proved the concept of running IDS inside the cloud, it was later discovered by that this arrangement is vulnerable to zero-day attacks. More information on zero-day attacks can be found in [15].

 

In [16], a new model for the detection of flooding based DoS attack on cloud environment was presented. The suggested model, which relies on covariance matrix, has three phases of execution. In the first phase, a baseline profile is created for normal traffic pattern. Intrusion detection occurs in the second phase and intrusion preventions takes place in the third phase. Although the paper did not include a clear comparison with other similar systems, it has shown good detection ability, especially in IaaS model.

A mOSAIC-based framework for providing a distributed intrusion detection system in the cloud was proposed in [17]. The suggested architectural framework collects information from different architectural levels in the cloud system. This information is collected using dynamically-deployed security components as a distributed architecture. Due to the distribution of the components, the suggested system allows monitoring different symptoms of DoS attacks on different architectural levels. The system presented in this paper is very promising as the prototype used in testing showed signs of success.

Research was done in [18] to employ a pattern-based approach to study defense mechanisms against DoS attacks in a model-based setting. In this paper, two formal patterns were introduced which can serve as defense against DoS attacks; adaptive selective verification pattern defending against DoS, and server replicator pattern in a cloud setting. In this paper, a formal pattern-based approach to the design and mathematical analysis of security mechanisms of cloud services was discussed. The proposed system showed signs of improvement in DoS attack detection.

In general, data center networks are typically under-provisioned. Although this does not seem to be a problem in a corporate data center, it might cause trouble in a shared infrastructure like cloud computing. A new DoS attack the aims at exploiting the network under-provisioning in a cloud infrastructure was introduced in [19]. The paper has proved that such an attack is practically implementable on cloud infrastructure. The paper also introduced a mechanism to detect and avoid this new form of attack.

A proposal was made in [20] to enhance cloud computing security, including resistance to DoS and DDoS attacks, through the architectural support of multiple hypervisors over a single platform. One of the results of having such architecture, named MultiHyp, was that the vulnerabilities of one hypervisor or its guest virtual machine would not spread outside its own domain. This gives the platform better resilience to malicious attacks and failures in the cloud. The suggested system employs a new cache eviction policy and memory management scheme to prevent resource monopolization on shared cache and physical memory.

As explained in [21], network intrusion detection systems can have high false-positives and they can impact performance. In this paper, multiple IDSs are deployed in each layer of the cloud infrastructure to protect virtual machines against threats, and mostly DoS and DDoS. The system proposed in this paper was tested through simulation and the results indicated higher detection rate and lower false-positive rate when compared to other systems.

In [22], a comber approach for security services, named the filtering tree, was introduced. The proposed system focuses on detecting DDoS attacks that operate at the application level. Specifically, XML, and HTTP DDoS attacks to services like Amazon E2C and Windows Azure were examined in this paper. The filtering tree proposed in this paper was composed of five filters to detect and resolve XML and HTTP DDoS attacks.

A proposal was made in [23] to adopt a hierarchical storage technique for maintain hop-count to prevent DDoS attacks in the cloud environment. DDoS attacks are usually accompanied by IP spoofing to hide the flooding source. This paper uses hop-count to assist in detecting flooding attacks. Although the proposed system is not experimentally easy to implement, it shows improvement in terms of identifying packets that come from a single source of a flooding attack despite the fact that the source IP address is spoofed.

The drawbacks of the current schemes used for handling DDoS were identified in [24]. The paper also proposes also a new direction in which the same level of security capabilities can be obtained in the network with minimal expense of resources. The paper shows experiments' results for a prototype implementation of the proposed concept with detailed description of the experimental setup.

 

### *4.3. Cloud-to-Outside*

Due to the dynamic nature of the cloud system, it can be very tempting for attackers to use cloud services to attack their targets. In [25], a cloud-oriented intrusion detection system was introduced. A thorough discussion on how to prevent using the cloud as an attacking platform to attack other DDoS targets was presented in this paper.

More information about DoS and DDoS attacks in the cloud can be found in [26,27,28,29,30]

## 5. Conlcusion

DoS and DDoS attacks pose a threat to availability of vast types of networking services. DDoS attacks always take great media attention with their growing magnitude and public exposure. The dynamic nature of cloud computing makes it susceptible to DDoS even more. The harm caused by DDoS on cloud computing is higher as compared to “classic” computing models.

In this paper, we discussed the basics of DDoS and cloud computing. The paper included discussion of recent research in the field of cloud DDoS detection and prevention.

## References

[1] Shui Yu, *Distributed Denial of Service Attack and Defence*. London, UK: Springer, 2014.

[2] Mike Lenon. (2014, February) CloudFlare Infrastructure Hit With 400Gbs NTP-Based DDoS Attack. [Online]. http://www.securityweek.com/cloudflare-infrastructure-hit-400gbs-ntp-based-ddos-attack

[3] Malachi Kenney. (1996, October) Ping of Death. [Online]. http://insecure.org/sploits/ping-o-death.html

[4] Richard Hill, Laurie Hirsch, Peter Lake, and Siavash Moshiri, *Guide to Cloud Computing: Principles and Practice*. London: Springer, 2012.

[5] Top-Threats-Working-Group, "The Notorious Nine: Cloud Computing Top Threats in 2013," Cloud Security Aliance, 2013.

[6] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in *Proceedings of the 16th ACM conference on Computer and communications security* , Chicago, 2009.

[7] Adam Bates et al., "Detecting Co-Residency with Active Traffic Analysis Techniques," in *Proceedings of The ACM Cloud Computing Security Workshop CCSW 2012*, Raleigh, 2012.

[8] Harkeerat Singh Bedi and Sajjan Shiva, "Securing Cloud Infrastructure Against Co-Resident DoS Attacks Using Game Theoretic Defense Mechanisms," in *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* , CHENNAI, 2012.

[9] Joseph Idziorek, Mark Tannian, and Doug Jacobson, "Detecting Fraudulent Use of Cloud Resources," in *Proceedings of The ACM Cloud Computing Security Workshop CCSW'11*, Chicago, 2011.

[10] Ryan Shea and Jiangchuan Liu, "Understanding the impact of denial of service attacks on virtual machines," in *Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service* , Hong Kong, 2012.

[11] Alina Mădălina Lonea, Daniela Elena Popescu, Octavian Prostean, and Huaglory Tianfield, "Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud," in *Proceedings of the 5th International Workshop Soft Computing Applications (SOFA)*, Szeged, 2012.

[12] Kazi Zunnurhain, "FAPA: A Model to Prevent Flooding Attacks in Clouds," in *Proccedings of ACMSE'12*, Tuscaloosa, 2012.

[13] Chirag Modi, Dhiren Patel, Bhavesh Borisanya, Avi Patel, and Muttukrishnan Rajarajan, "A Novel Framework for Intrusion Detection in Cloud," in *Proceedings of 5th International Conference on Security of Information and Networks (SIN 2012)*, Jaipur, 2012.

[14] A. Bakshi and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," in *Proceedings of Second International Conference on Communication Software and Networks, 2010. ICCSN '10.*, Singapore, 2010, pp. 260-264.

[15] R. Lippmann, J. W. Haines, D.J. Fried, J. Korba, and K. Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation," *Journal of Computer and Telecommunications Networking - Special Issue on recent advances in intrusion detection systems*, vol. 4, pp. 579–595, 2000.

[16] Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, and AAmir Shahzad, "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach," , Kota Kinabalu, 2013.

[17] Massimo Ficco, Salvatore Venticinque, and Beniamino Di Martino, "mOSAIC-Based Intrusion Detection Framework for Cloud

 

Computing," in *Proceedings of Confederated International Conferences: CoopIS, DOA-SVI, and ODBASE 2012*, Rome, 2012, pp. 628-644.

[18] Jonas Eckhardt, Tobias Muhlbauer, Musab AlTurki, Jose Meseguer, and Martin Wirsing, "Stable Availability under Denial of Service Attacks through Formal Patterns," in *Proceedings of 15th International Conference on Fundamental Approaches to Software Engineering (FASE)*, Tallinn, 2012.

[19] Huan Liu, "A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, Chicago, 2010.

[20] Weidong Shi, JongHyuk Lee, Taeweon Suh, Dong Hyuk Woo, and Xinwen Zhang, "Architectural Support of Multiple Hypervisors over Single Platform for Enhancing Cloud Computing Security," in *Proceedings of the 9th conference on Computing Frontiers CF'12*, Cagiliari, 2012.

[21] Huaibin Wang and Haiyun Zhou, "The Research of Intrusion Detection System in Cloud Computing Environment," in *Proceedings of the 2011 International Conference on Multimedia, Software Engineering and Computing*, Wuhan, 2011, pp. 45-49.

[22] Tarun Karnwal, Sivakumar Thandapanii, and Aghila Gnanasekaran, "A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack," in *Proceedings of the International Symposium on Intelligent Informatics ISI'12*, Chinnai, 2012.

[23] Vikas Chouhan and Sateesh K. Peddoju, "Hierarchical Storage Technique for Maintaining Hop-Count to Prevent DDoS Attack in Cloud Computing," in *Proceedings of International Conference on Advances in Computing*, Karnataka, 2012.

[24] Sanchika Gupta and Padam Kumar, "VM Profile Based Optimized Network Attack Pattern Detection Scheme for DDOS Attacks in Cloud," in *Proceedings of International Symposium on Security in Computing and Communications (SSCC'13)*, Mysore, 2013, pp. 255-261.

[25] Frank Doelitzscher, Christoph Reich, Martin Knahl, Alexander Passfall, and Nathan Clarke, "An agent based business aware incident detection system for cloud environments," *Journal of Cloud Computing*, vol. 1, no. 1, December 2012.

[26] Nelson Gonzalez et al., "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing*, vol. 1, no. 1, December 2012.

[27] Huiming Yu, Nakia Powell, Dexter Stembridge, and Xiaohong Yuan, "Cloud Computing and Security Challenges," in *Proceedings of 50th ACM Southeast Regional Conference SE'12*, Tuscaloosa, 2012, pp. 298-302.

[28] Duygu Sinanc and Seref Sagiroglu, "A Review on Cloud Security," in *Proceedings of The 6th International Conference on Security of Information and Networks*, Aksaray, 2013, pp. 321-325.

[29] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561-592, February 2013.

[30] S. Ramgovind, M.M. Eloff, and E. Smith, "The management of security in Cloud computing," in *Proceedings of 2010 Information Security for South Africa (ISSA)*, Johannesburg, 2010, pp. 1-7.

 