An Architecture for Detecting Information Technology Infrastructure Policy Violations in a Cloud Environment

Ruth Anyango Oginga,
School of Science, Enginnering & Technology, Kabarak University

Felix Musau
School of Computing Sciences, Riara University, Kenya

Christopher Maghanga
School of Science, Enginnering & Technology, Kabarak University

Corresponding author: roginga@kabarak.ac.ke

Abstract

Organizations are increasingly becoming aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Just like any other technology it brings new security threats and challenges. A smooth transition entails a thorough understanding of the benefits as well as challenges involved. Privacy is a concern that has risen as obstacle to widespread adoption of clouds by users. Many organizations consider the deployment of different types of protection systems to curb the various malicious activities. The systems can offer sophisticated monitoring and reporting capabilities to identify attacks against cloud environment, while stopping multiple classes of attacks before they are successful against a network. Despite the use of protection systems to detect any malicious activities, some users still find ways to violate some of the laid down IT infrastructure Acceptable Use Policies. While many cloud security research focus on enforcing standard access control policies typical of centralized systems, such policies have often proved inadequate. For this reason, an architecture has been developed to automatically detect IT infrastructure policy violation in a cloud environment The implication of this research is that institutions would regain their trust in this paradigm and consider implementing policies in their clouds. Since policy violation is one of the major hindrances to the implementation of cloud computing, the policy violation detection architecture could be employed by institutions to ensure data security in cloud environment. The architecture uses software agents as its core components to collect evidence across cloud environment. The architecture captures any policy violation in the cloud environment when using any IT infrastructure. Therefore we discuss the policy violation detection architecture and present our findings in this paper.

Keywords: Architecture, Policy violation, IT infrastructure, Cloud environment, Detection

I. INTRODUCTION

So many organizations today make use of Acceptable Use Policy to specify the actions prohibited to the users of an organization’s IT infrastructure. Recent cloud computing models are known to be very promising internet-based computing platforms, however these models could result in a loss of security over customer data. This usually happens because the enterprise IT assets are hosted on third-party cloud computing platforms.

All users are usually required to adhere to all the policies specified in the acceptable use policy document without exception. Despite the use of intrusion detection system (IDS) is not guaranteed and cannot be considered as complete defense, the researcher believe it can play a significant role in the Cloud security architecture (Mchugh, 2000).

For this reason architecture would assist network administrators to automatically detect policy violation by gathering relevant evidence data from the node and other IT infrastructure on a cloud environment. Policy violation detection architecture provides prevention capabilities rather than just detection so it can further stop the attack itself as noted by terminating the user session that is being used for the attack, block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute, or block all access to the targeted host, service, application, or other resource. This allows the user to have self-discipline when accessing or using cloud environment.

II. RELATED WORK

There are several studies have been conductedpreviously that aimed to integrate IT functions of Public/private University cloud computing. Most of the paperdiscussed private cloud computing, others public cloud computing and others hybrid. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided. To begin with, Examined about cloud computing, and a new model is introduced for cloud computing (Wyld 2010).

Vaquero (2011) focused on the effectiveness of using services cloud such as IaaS and PaaS in educational fields, especially in teaching advanced Computer Science courses. By Praveena and Betsy (2009) provided a comprehensive introduction to the application of cloud in university.

The proposed service support for campus Cloud, in which all resources are virtualized into service based on the virtualization technology, could achieve resource sharing in campus Cloud system. The service pool provides the necessary support for integration of local resources and technology environment for a variety of scattered resources, under the existing conditions to meet the users in universities.The campus cloud platform must need to give special service support for users (Ye and Chen 2011).

However, the software’s are installed once, and job scheduling will control the same type of job to the respective cloud servers. To provide virtualization techniques, the cloud servers are referred to as node controller and deploy hypervisors. Local server would act as a (middleware) cluster controller containing warlrus, storage controller and session controller. The Middleware use honey bee algorithm, active clustering, and biased random sampling algorithms. Further, the local server also resolves the primary authentication and access control

Level of awareness on policies in cloud environment

Despite all those IT policies and restrictions, that staff is aware of; staff wants to use personal devices for work because it allows them to be more productive. Agreeing to these IT enforced policies usually give workers the ability to access company emails, use remote desktop tools or virtualization to access their files (Schulz, 2016). An interesting finding is that only one third of staff reported about their knowledge of solutions for data protection in the cloud. This finding indicate a pattern that to an extent cloud service users are aware of privacy and security issues when storing their data, although they are less aware of solutions related to these issues. Similar results are found in which showed that there is an alarmingly high percentage of users from

Switzerland and India, who are not aware that the CSPs obtain the right to modify user data and disable user accounts at any time (Sachdeva et. al., 2011).

This outcome is derived as a result of the fact that users do not read policies violations and terms of service of the cloud services they use. In another study the Australian respondents believed that the cloud computing made it more difficult for organizations to find a way to protect customers' data and the greatest concern was regarding the risk of losing control over data locations and data unauthorized access (Quah,2013).

This possesses serious concerns from a user perspective; organizations lose control over their vital data and are not aware of any security mechanisms put in place by the provider having data in an unknown place and with no control over it are one of the leading concerns to organizations when switching to cloud computing (Behl, 2011).

Causes of policy violation

Federation defense approach, in which the IDSs are deployed in each Cloud computing region, IDSs cooperate with each other by exchanging alerts, and implement a judgment criterion to evaluate the trustworthiness of these alerts. A cooperative component is used to exchange alert messages from other IDSs. Majority vote method is used for judging the trustworthiness of an alert (Chi-Chun et. al,2010).

Lack of policies and standards

Network administrators often give staff policies the benefits of doubt because employees don't always break the rules of malicious or vindictive reasons. Rather workers may not even know that certain actions break company's' policy. Breaches can occur when employees store company information in third party cloud services or when they use a blacklisted app, jail broken phone or other devices that does not meet the company guidelines employees who violate policies usually do so to be more productive (schulz, 2016).

Theft of Service Attacks

The Theft of Service attack utilizes vulnerabilities in the scheduler of some hypervisors. The attack is realized when the hypervisor uses a scheduling mechanism, which fails to detect and account of Central Processing Unit (CPU) usage by poorly behaved virtual machines. This failure may further allow malicious customers to obtain cloud services at the expense of others. This attack is more relevant in the public clouds where customers are charged by the amount of time their VM is running rather than by the amount of CPU time used. Since the Virtual Machine Manager (hypervisor) schedules and manages virtual machines, vulnerabilities in the hypervisor scheduler may result in inaccurate and unfair scheduling. These vulnerabilities mainly result from the use of periodic sampling or low-precision clock to measure CPU usage: like a train passenger hiding whenever ticket checkers come for tickets (Fangfei, 2011).

Mechanisms to enable self- protection of the cloud infrastructure

Dynamic service provisioning using GRIA SLAs, The authors describe provisioning of services based on agreed SLAs and the management of the SLAs to avoid violations. Their approach considers only Grid environments and not Clouds.

Firewall

Firewall is a combination of hardware and software that isolates an organization's internal network from other networks, allowing some packets to pass and blocking others. It functions to avoid unauthorized or illegal sessions established to the devices in the network areas it protects. Firewalls are configured to protect against unauthenticated interactive logins from the outside world. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Basically, numbers of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in depth network security protection. Administrators that manage the firewalls have a have to be careful while setting the firewall rules (Bourducen et. al., 2009).

Intrusion Detection System (IDS)

Intrusion Detection System helps information systems to deal with attacks. This is accomplished by collecting information from a variety of systems and network sources. The information collected is analyzed for possible security problems. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. The intrusions may include attacks both from outside the organization as well as within the organization (Samrah, 2003).

Cyberoam

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions. Cyberoam's perfect blend of best-of-breed solutions includes Identity based Firewall, Content filtering, Anti-Virus, Anti-Spam, Intrusion Detection and Prevention (IDP), and VPN. Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection. It also provides assistance in improving Bandwidth management, increasing Employee productivity and reducing legal liability associated with undesirable Internet content access.

POLICY VIOLATION DETECTION ARCHITECTURE

The user can access the POVIDA using different technologies such as laptops and phones. The user can access different cloud services depending on cloud service providers. These serviced are put in layers. The upper layer is Software as a Service (SaaS), which is the one visible to the final user and involves applications. The next layer is Platform as a Service (PaaS) and it matters to software developers. It is composed by the operating systems, application programming interfaces (API), documentation, and basic services. Infrastructure as a Service (IaaS) refers to the usage of available resources on the cloud: memory, processors, storage and finally business process as a service (BPaaS) as the delivery of business process outsourcing (BPO) services that are sourced from the cloud and constructed for multitenancy. As a cloud service, the BPaaS model is accessed via Internet-based technologies. A cloud management platform is a suite of integrated software tools that an enterprise can use to monitor and control cloud computing resources. While an organization can use a cloud management platform exclusively for a private or public cloud deployment, these toolsets commonly target hybrid and multi-cloud models to help centralize control of various cloud-based infrastructures. Then there is policy violation detection architecture that is used to detect any violation on the cloud see figure 1.

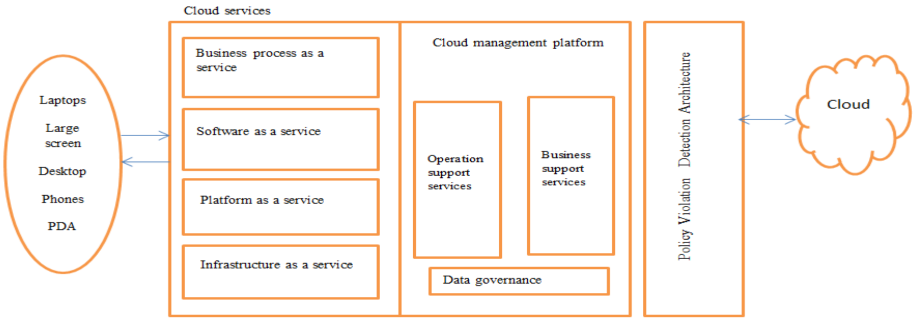
Cloud services
Laptops
Large screen
Desktop
Phones
PDA
Business process as a service
Software as a service
Platform as a service
Infrastructure as a service
Cloud management platform
Operation support services
Business support services
Data governance
Policy Violation Detection Architecture
Cloud

Figure 1: Policy violation detection architecture

III METHODOLOGY

There exist different approaches that have been used in the security of data in the network. In this paper, though Design science research methodology and descriptive research design was used in this study. Descriptive research is a study designed to depict the participants in an accurate way and describes people who took part in this study (Kowalczyk, 2015). This approach was used to analyse and define the policy violation in the cloud environment. This involved closed ended questionnaires to collect views of users in the institutions. Descriptive survey was therefore chosen for this study because of the opinions of the respondents in terms of security in cloud computing. Descriptive research design enabled the study to generalize the findings to a larger population.

Population of the Study

The targeted population for the study was the five Universities in Kenya. This target population has been chosen purposively for this research because these Universities have sensitive and crucial data that needs to be kept secure and private as well as utilize IT infrastructures for growth. The Universities consist of those in the staff, students and Managements who are currently using cloud computing or considering the use of cloud computing due to their infrastructure size and requirement. The Universities had a focus group of people who participated in the research that filled in the questionnaires. These included the ICT managers, Staff in the department of computer Science, Fourth year students in the department computer Science and Network Administrators.

Pilot Experiment

Experimental method was used to attempt to detect any IT infrastructure policy violation in the cloud. There were a number of times that the architecture was tested and it was worked well. Seventy (70) participants also tested the architecture and were observed. It was testing whether the architecture was testing the violation in cloud. Data collected from the survey was checked for completeness, consistency, accuracy and uniformity. The regression analysis approach was used to analyze the data collected in order to examine the relationship between two or more variables of interest. It studies the influence of one or more independent variables on a dependent variable. Data entry, descriptive, graphical, reliability and regression analysis was done using minitab version17. This helped in explaining between the variable and which variable was more important than the other. An initial coding framework with the list of themes was first developed. By applying analytical and theoretical ideas developed during the research, these themes were refined and reduced by grouping them together. This list formed the final category that was used to produce a list used to violate policies. Chi square was used to analyze the data on each objective.Chi-Square test of independence is used to determine if there is a significant relationship between two categorical variables.

III. FINDINGS

Data was collected using a survey and observation on the developed architecture. The survey purpose was to know the level of awareness of users towards cloud computing and the needs of users, while the observation was intended to confirm if the needs and requirement were met on the development of the architecture. The survey was done in different institutions and the architecture was done by different group of people. The response rate was ninety five (95) out of one hundred and two (102), and seventy (70) people tested the architecture. The results are summarized in Table 1 about (42%,) of the respondents strongly agreed that the institution have strict policies on what can be accessed and what cannot be accessed on the cloud. Majority of the respondents (43%) also agreed that cloud services providers through network admin analyses the logs with response rate of 67%. The results of the respondents (63%) also significantly strongly agreed and agreed) that Policies in place conform to legal requirement. The findings also revealed that penalties are clearly outlined for violation of policies 61% of the respondents (strongly agreed and agreed).The results of the respondents (60%) significantly(strongly agreed and agreed) thatPolicy violation detector analyses the operations to determine whether it violates data loss prevention policy. When respondents were asked whether Policy violation detector analyses the content that is either accessed or saved onto any storage system, (34%) agreed. Policy violation detector monitors users actions by intercepting with (54%) approval.

Table 1: Policy violation

	SD(%)	**D(%)**	**UN(%)**	**A(%)**	**SA(%)**	X^2	**Pr>** X^2
The institution have strict policies on what can be accessed and what cannot be accessed on the cloud	2.02	7.07	15.15	33.33	42.42	59.1	<.0001
Cloud services providers through network admin analyses the logs	1.01	4.04	27.27	43.43	24.24	61.2	<.0001
Policies in place conform to legal requirement	1.03	8.25	27.84	32.99	29.9	40.1	<.0001
Penalties are clearly outlined for violation of policies	3.06	9.18	26.53	36.73	24.49	37.0	<.0001
Policy violation detector analyses the operations to determine whether it violates data loss prevention policy	1.02	9.18	29.59	38.78	21.43	45.3	<.0001
Policy violation detector analyses the content that is either accessed or saved onto any storage system	3.03	9.09	33.33	34.34	20.2	39.1	<.0001

Policy violation detector monitors users actions by intercepting	3.13	12.5	30.21	25	29.17	26.6	<.0001

Regression analysis results

The regression analysis approach was used to analyze the data collected in order to allow the study to examine the relationship between two or more variables of interest. It examines the influence of one or more independent variables on a dependent variable.

Regression Analysis

The regression equation is

$$y = 3.91 + 0.103x1 + 0.213x2 + 0.591x3$$

Analysis of Variance

Table 2.Analysis of variance

Source	DF	SS	MS	F	P
Regression	3	1272.13	424.04	26.54	0.000
Residual Error	95	1517.89	15.98		
Total	98	2790.02			

S = 3.99722 R-Sq = 45.6% R-Sq(adj) = 43.9%

IV. CONCLUSION AND FUTURE WORK

Today, cloud computing is being defined and talked about across the ICT industry under different contexts and with different definitions attached to it. However, despite the flow in activity and interest, there are significant, persistent concerns about cloud computing that are hindering the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Additional concerns regarding privacy and security were also established and addressed through enhancements to the architecture and prototype. The research found out that most respondent was not sincere in the survey because they could imagine and indicate instead of what they really knew. The respondents were asked whether their institution have strict policies on what can be accessed and what cannot be accessed. The study found out that the majority were aware that there are policies in place. In real sense there are no outline policies in place. This was not achieved but in the recommendation it was suggested that institutions to outline penalties and conform to legal requirements. POVIDA is able to analyses policy to determine policy violation and it can also analyses the content being accessed and before saving the data. It can also monitor the users' actions by blocking.In future the studies should explore the possibility of providing suitable frameworks for capturing of screen short in cases where policy violation is detected.

REFERENCE

Barinder, K. and Sandeep, S. (2014) 'Parametric Analysis of various Cloud Computing Security Models', *International Journal of information and Computation Technology.*, vol. 4, no. 15, 2014, pp. 1499-1506.

Becker, J.D. and Elana, B. (2014) 'IT Controls and Governance in Cloud Computing', 20th Americas Conference on Information systems(AMCIS), Savanah.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Information and communication technologies (WICT), 2011 world congress on (pp. 217-222).IEEE.

Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS).International Journal of engineering and information Technology, 2(1), 60-63.

Computing, C. (2010). Security–A Natural Match.Trusted Computing Group (TCG) http://www. trustedcomputinggroup. org.

S. Pearson and T. Sander (2010),“A mechanism for policy-driven selection of service providers in SOA and cloud environments,” in Proceedings of the 10th Annual International Conference on New Technologies of Distributed Systems (NOTERE '10), pp. 333–338.

V. C. Emeakaroha, M. A. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. deRose, (2012) “Towards autonomic detection of SLA violations in cloud infrastructures,” Future Generation Computer Systems, vol. 28, no. 7, pp. 1017–1029.

Vaquero, L.M. (2011). EduCloud: PaaS versus IaaS Cloud Usage for an Advanced Computer Science Course. IEEE Transactions on Education. [Online]. 54 (4). pp. 590–598. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5686886.

Y. Chi, H. J. Moon, H. Hacigümüş, and J. Tatemura,(2011) “SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing,” in Proceedings of the 14th International Conference on Extending Database Technology: Advances in Database Technology (EDBT '11), pp. 129–140.