Evaluation of mechanisms that enable self- protection on policy violation in cloud Infrastructure

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
Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012). However, as the shape of the cloud computing is emerging and developing rapidly both theoretically and in reality, the cloud security, data and cloud infrastructure and privacy issues still pose significant challenges. It still lacks mechanism to enable itself from policy violation.In this work, we describe various mechanisms that would enable self-protection on policy violation in cloud infrastructure. In particular, we discuss five critical mechanisms: IDS, Cyberoam, Federated Identity Management System, firewall and honeypot. Some solutions to mitigate these attacks on these mechanisms are also proposed along with a brief presentation on the future trends in cloud computingdeployment. Finally we evaluate these mechanisms based on the data collected from users in case they know how to protect their data in cloud environment.

Keywords: Policy violation, cloud infrastructure, evaluating and self-protection

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. 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).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. Moreover, they do not detail how the low-level metric are monitored and mapped to high-level SLAs to enforce the SLA objectives at runtime. Moreover, with the rapid

changing technology environment it is clear that, more speedy changes in the way security incidences are detected and the way security data is analyzed needs to be done (Markus et. Al., 2012). This paper, therefore, presents mechanisms that enable self- protection on policy violations in cloud infrastructure. The primary objective is to evaluate the mechanisms that enable self- protection on policy violation in developed tools and techniques that can be part of cloud infrastructures to detect policy violations. This paper is made up of:- Introduction, related studies, critical mechanisms, future trend in cloud computing, evaluation mechanisms to enable self- protection in cloud and finally conclusion and future work.

RELATED STUDIES

There exists various research works from different scholars which have made valuable contributions towards the study in this paper. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided. Discussion on autonomous QoS management using a proxy-like approach, their implementation is based on WS-Agreement. Thereby, SLAs can be exploited to define certain QoS parameters that a service has to maintain during its interaction with a specific customer Also, their approach is limited to Web services and does not consider other applications types (Koller and Schubert 2007)

In an effort towards fighting IT infrastructure policy violations and collect relevant incidence information in a LAN environment, law enforcement agencies have also started incorporating the collection and analysis of digital evidence data into their infrastructures. However they do not consider application deployment and provisioning strategies (Dobson and Sanchez 2011).

Creating a security policy is the first step in protection and enforcement. While it may seem excessive, enterprises need to define which assets users are entitled to access and under what conditions as well as which resources and applications are prohibited. Especially important is establishing individual accountability. Beth Israel Deaconess Security policy details everything from the protection of confidential information to large files transfers, misuse of software, protection of passwords and malware prevention. Increasing awareness about the risks resulting from unchecked trust is resulting in stronger more visible security policies, rather than allowing acceptable use policies and non-disclosure agreements to dictate consequence of inappropriate actions. Organizations are drafting policies that specifically list misuse of computer equipment and data as an offense that can result in punitive actions including termination (Anon, 2014).

According to Bruneton et al. (2006) demonstrated the viability of component-based design to build complex systems from heterogeneous building blocks and reach flexible security. We explore that approach to orchestrate and adapt security services in a cloud (e.g., as Web Services) to compose individual security services flexibly inside a unified security architecture. Security properties provided by individual security services are expressed as flexible contracts, e.g., Service-Level Agreements, to derive overall security objectives guaranteed by the cloud infrastructure.

Computing approach for self-managed security also proved its interest to build security infrastructures with minimal security administration overheads. It satisfies multiple security requirements, and reacts rapidly to detected threats: security parameters are autonomously

negotiated with the environment to match the ambient estimated risks and achieve an optimal level of protection (Chess, 2003). A first generic component-based framework for self-protection has been defined Lacoste et al. (2010). The first part of this dissertation work study whether this framework is sufficient for self-management of cloud security, and define the necessary extensions for that purpose.

Critical mechanisms

There five critical mechanisms to enable self- protection in cloud infrastructure these are IDS, Cyberoam, federated Identity management, firewall and honey pot.

Intrusion Detection Systems

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.

Federated Identity Management System

The backbone of cloud computing security is tightly coupled with identities used to access cloud infrastructure. Management of identities (IDM) is about maintaining the integrity of identities, throughout their life cycle, to make it and its related data (e.g., authentication and authorization results) available to different services in secure and privacy-protected manner (Bishop, 2002). The concept of federated identity management (FIM) is about managing identities by allowing an identity subject to establish links between his/her identities, each of which can be used for a different service, across geographical and organizational borders (Bishop 2002). Establishing a logical link between identities is called identity federation. The federation is a group of organizations that establish trust among themselves in order to cooperate safely in business (Leandro, 2012).

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 (Benkhelifa et. al., 2009).

Honeypot

Honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. A honeypot works by fooling attackers into believing that it is a legitimate system. The attackers attack the system without knowing that they are being observed. When an attacker attempts to compromise a honeypot, its attack related information, such as the IP address of the attacker, will be collected. This activity done by the attacker provides valuable information and analysis on attacking techniques, allowing system administrators to trace back to the source of attack if required (Levin & Labella 2003)

In general honeypots can be divided into two categories. Production Honeypots:Production honeypots are used to assist an organization in protecting its internal IT infrastructure. These secure the organization by policing its IT environment to identify attacks. These honeypots are useful in catching hackers with criminal intentions. The implementation and deployment of these honeypots are relatively easier than research honeypots because these have less purpose and require fewer functions. As a result, they also provide less evidence about hacker‟s attack patterns and motives. Research Honeypots: Research honeypots are complex. They are designed to collect as much information as possible about the hackers and their activities. Their primary mission is to research the threats organization may face, such as who the attackers are, how they are organized, what kind of tools they use to attack other systems, and where they obtained those tools. While production honeypots are like the police, research honeypots act as their intelligence counterpart and their mission is to collect information about the attacker. The information gathered by research honeypots helps the organization to better understand the hackers attack patterns, motives and how they function (Zhan et. al., 2013).

FUTURE TRENDS IN CLOUD COMPUTING
Growth in Cloud Services Solutions

Cloud computing future growth all began when the growth of infrastructure as a service, IaaS, and platform as a service, PaaS, expanded the number of cloud solutions available in public and private sectors. As IaaS and PaaS continue to be used worldwide to achieve diverse goals, we will see these solutions as the most deployed cloud services around the world. Cisco predicts that SaaS, software as a service, solutions will account for more than 60% of all cloud-based workloads this year. They also predict that PaaS and IaaS solutions will increase throughout

2018. Any business looking to simplify their operations and make services easier to access for customers will most likely move toward cloud services solutions.

Increased Storage Capacity

A huge aspect affecting the future of cloud computing is the amount of storage cloud computing will offer companies and individuals. This growth is because many businesses are adopting cloud technology as a huge part of doing business. It is predicted that providers will bring more data centers online with larger-capacity storage equipment throughout this year. Cisco estimates the storage capacity of the cloud will double this year alone. With this increased storage, more businesses will be able to store large data sets and perform analytics using cloud computing. Being able to perform analytics on this massive amount of data will allow companies to gain valuable insights into customer behavior, human systems, and strategic financial investments, just to name a few.

Introduction of the Internet of Everything (IoE)

Most of us have heard the buzzword, internet of things, IoT. With continuous innovations in real-time data analytics and cloud computing, we will see the newest technology buzzword, internet of everything, be used more often as 2018 progresses. Cloud computing will play a major role in the way IoE develops as it relies heavily on machine to machine communications, data, processes and the way humans interact with things in their environment. A major trend we will see this year is the significant role cloud computing will play in IoE's ability to simplify all interactions.

Enhanced Internet Quality

The quality of the internet has been getting immensely better every year since it was created. 2018 is expected to be no different, as the amount of data generated and stored around the world increases. Customers today already expect high-quality, fast-loading services and apps and this expectation will enhance network quality and cloud computing. This high-quality expectation will also lead businesses to upgrade their platforms and services to be more responsive to the needs of their customers. As the quality of the internet is enhanced, IoT and IoE industries will benefit a great deal from the faster network speeds and the ability to receive and deliver data more efficiently in real time.

Cloud Solutions to Security Challenges

One of the most important cloud computing trends 2018 will see is the increased solutions the cloud will bring to security. 2017 saw the most cyber-attacks ever recorded in the history of the internet and 2018 should be no different. Many experts predict 2018 will see more individual and state-sponsored attacks aimed at undermining cloud infrastructure security. Cyber-attacks are also becoming more sophisticated which means anyone in charge of their company's security will need to become more sophisticated in the way they detect and prevent these attacks. Cloud services will be able to help companies with their security measures by offering managed security services

EVALUATING MECHANISM TO ENABLE SELF- PROTECTION IN CLOUD INFRASTRUCTURE

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.

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 where Respondents never agreed on whether data/information on transit

is always safe regardless of the deployment model used. They never agreed that the architecture allows unauthorized access to data/information in the cloud. Respondents (strongly agreed and agreed) 65%, those hackers can manipulate weakness in data security model to get an illegitimate access to data or application. Majority of the respondents also strongly agreed 45% that applications created without policies followed are potential security risks due to incompatibility and integration issues, there is only (2%) who strongly disagreed. Respondents (strongly agreed and agreed) 79%,that Intrusion Detection System approach also improves security by helping to capture the overall extent of an attack. Minority of the respondents strongly disagreed 2%, that the architecture contain both detection and reaction mechanisms this was supported .When the respondents were asked if all monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture, majority of the respondents strongly agreed and agreed49%, that all monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture.

Table 1: Mechanisms to enable self-protection of the cloud infrastructure

	SD(%)	D(%)	UN(%)	A(%)	SA(%)	χ^2	Pr> χ^2
Data/information on transit is always Safe regardless of the deployment model used.	12.12	14.14	36.36	18.18	19.19	18.2	0.0011
The architecture allows unauthorized access to data /information in your cloud.	14.14	27.27	16.16	27.27	15.15	8.8	0.0655
Hackers can manipulate weakness in data security model to get an illegitimate access to data or application	9.09	6.06	20.2	40.4	24.24	37.0	<.0001
Applications created without policies followed are potential security risks due to incompatibility and integration issues.	2.04	4.08	15.31	33.67	44.9	68.8	<.0001
Intrusion Detection System approach also improves security by helping to capture the overall extent of an attack	2.02	4.04	15.15	41.41	37.37	67.4	<.0001
The architecture contain both detection and reaction mechanisms	2.02	6.06	32.32	37.37	22.22	48.3	<.0001
All monitoring operations are done outside the virtual machines so the attacker cannot modify the architecture	3.06	10.2	37.76	27.55	21.43	37.1	<.0001

CONCLUSION AND FUTURE WORK

Security measures should be dynamic and autonomous. Cloud computing infrastructure is changing fast requiring security measures and policies to be updated regularly at the same pace to match the changing behavior of the clouds. Furthermore, licensing is crucial to the security of clouds. Standard policies should be strictly implemented in clouds and organizational/governing bodies should visit clouds' staff and infrastructure on regular bases to evaluate the efficiency of the security precautions adopted by the purveyors. The statistics for attacks, occurring in any cloud, should be publically available to determine the reliability of cloud purveyors. This type of

sharing helps other cloud's security experts to guard against new attacks. Also, it is extremely important to holistically investigate the various cloud security related parameters including risks, threats, challenges, vulnerabilities, and attacks. The mechanisms chosen should at all cost self-protect you when you are using cloud. The possibility of being attacked can be reduced by deeply understanding the dependencies among these considerations. Finally, note that virtualization is a backbone of cloud computing. However, the concept of using virtualization in cloud computing is not yet mature as there are numerous number of attacks that target the virtualization environment. Examples of these attacks include information leakage during VM migration, service theft by manipulating VMs, uploading malicious VMs on cloud server, and rolling back VMs. Therefore, it is extremely important to develop reliable schedulers that, by design, contain sufficient security mechanisms. We have identified a few areas that are still unattended in cloud computing security such as auditing, and migration of data from one cloud to another which can be tackled in future.

REFERENCE

S. Bouchenak,(2010) "Automated control for SLA-aware elastic clouds," in Proceedings of the 5th International Workshop on Feedback Control Implementation and Design in Computing Systems and Networks (FeBiD '10), pp. 27–28.

Cappos, J., Beschastnikh, I., Krishnamurthy, A., & Anderson, T. (2009). Seattle: A platform for educational cloud computing. SIGCSE Bulletin, 41, 111-115

Malik, S., Huet, F. & Caromel, D. (2012). Cooperative cloud computing in research and academic environment using Virtual Cloud. In: 2012 International Conference on Emerging Technologies. [Online]. October 2012, Islamabad: IEEE, pp. 1–7. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6375445.

A. Samrah, "Intrusion Detection Systems; Definition, Need and Challenges," http://www.sans.org/reading_room/whitepapers/detection/intrusion detection systems-definition challenges_343, October 31, 2003.[8].

Bishop, M. *Computer Security: Art and Science*; Addison-Wesley Professional: Reading, MA,

Chou, T. (2013): security threats on cloud computing vulnarabilities, international journal of computer science & information technology (IUCSIT) vol. 5 No3.

E. Benkhelifa and T. Welsh, "Towards Malware Inspired Cloud Self-Protection," proceedings of the 2014 International Conference on Cloud and Autonomic Computing (ICCAC 14), 2014, pp. 1–2.

Leandro, M.A.P.; Nascimento, T.J.; dos Santos, D.R.; Westphall, C.M.; Westphall, C.B. Multitenancy authorization system with federated identity for cloud-based environments using

Leavitt, N. (2009) 'Is cloud computing really ready for prime time?',*Computer*, vol. 42, 2009, pp. 15- 20.

Levin, J. and Labella, R., "The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks", IEEE Proceedings, pp.92-99, 18 June 2003.[10]."Honeypot Security", http://www.infosec.gov.hk/english/technical/files/honeypots.pdf.[11].

Khorshed, M.T.; Ali, A.B.M.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Gener.Comput. Syst.***2012**, *28*, 833–851.

D. Chess, C. Palmer, and S. White. Security in an Autonomic Computing Environment. IBM Systems Journal,42(1):107–118,2003.Truehost.https://www.truehost.co.ke/cloud-providers-kenya/

Gartner (2012). Gartner Highlights Five Attributes of Cloud Computing. [Online]. 23 June. Available from: http://www.gartner.com/newsroom/id/1035013.