International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

Evaluating Causes of Policy Violation in Cloud Environment

Dr. Ruth Oginga
Lecturer,
Department of Computer Science and IT,
Kabarak University, Kenya

Dr. Nelson Masese
Lecturer,
Department of Computer Science and IT,
Kabarak University, Kenya

***Abstract*:- Organizations are increasingly becoming aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. With the diverseness of technologies, there are different security attacks and challenges. There are several important challenges that exist with regard to efficient provisioning and delivery of services through cloud. Threats on the cloud environment can be due to policy violation.Despite the use of protection systems to detect any malicious activities, policy violation is one factor that hinders widespread usage of cloud. The focus of this paper is on causes of policy violation that can affect the usage of cloud environment. In particular, the paper discusses four main causes of policy violation these are privacy, security regulatory and attacks on cloud. Some solutions to mitigate causes of policy violation were also discussed. This approach was evaluated by conducting a survey. The results were demonstrated using chi square. It was recommended that a strong security and applicable policy standard needs to be implemented and regulated more often. The global dimension of cloud computing requires standardized policy in each organization and practical solutions to enable stakeholders to assess their risks and establish adequate protection levels.**

Keywords: Policy violation, cloud, security

1. INTRODUCTION

Cloud computing is defined as both the applications dispersed as services over the Internet and the systems software and hardware in the data centers that offer those services (Zhang et.al., 2010).

The need for cloud computing was possibly necessitated by increased corporate information volumes beyond the convectional computer storage growing into thousands of Gigabytes over time. The distributive nature of businesses and systems and the reliance of data for performing most business operations mean data has to be available anywhere and anytime. Cloud computing is a platform that provides such flexibility of making data available on demand and is becoming a popular method of data storage as well as a service platform. Most importantly, cloud computing provides a storage facility that is hosted and accessible over the internet, making data readily available when and as required (Rimal et. al., 2009).

Cloud environment has become increasingly popular service due to the numerous advantages it possesses. These include high computing power, cheaper cost of services, better performance, scalability, and accessibility, the ability of cloud to access all your work, program and information from any device, and availability among others (Kundra 2011). However, since this kind of computing paradigm is fairly new, it has shortfalls that need to be addressed to make cloud computing services more convenient to use. Shortfalls include lack of policy standard, security issues and privacy. Security is viewed as one of the main adoption stoppers to cloud computing and the complexity of infrastructure involved leaves the door open to various threats coming from outside and within. Intrusions, malware or security policy violations of curious or malicious users are just but a few. Different network administrators use different types of network-based and host-based security software to detect malicious activities in cloud, the main target of the assailants is to make illegal and unauthorized attack to the presented resources in the Cloud computing settings.

There are different cloud computing service model used, as infrastructure as a service, platform as a service and software as a service According to Ramgovind et.al., (2010) to provide a secure Cloud computing solution, it‘s important to decide on the type of cloud to be implemented. Currently there are four types of cloud deployment models offered namely, public, private, hybrid and community.

Cloud computing has allowed and will allow even more seamless scaling of resources as the demand changes. In spite of the several advantages that cloud computing brings along with it, there are several concerns and issues which need to be solved before global demand of usage is realized. First, arises due to weak policy standards, thus putting the cloud environment at the risk of hacking and various attacks to cloud IT infrastructure. Moreover, transmission challenges of data to and from the cloud and privacy of data in the cloud environment requires round the clock monitoring. Therefore, one cannot just move applications to the cloud and expect them to run efficiently.

The research presents a survey to assess the causes of policy violation in the cloud environment. We want to find out what are some reasons to policy violation. The main objective is to assess the causes of policy violation using a survey.

The research instigates to introduce the cloud computing, cloud environment and security issues affecting cloud environment. The arrangement of the paper is as follows, section 2 present the related studies, section 3 present causes of policy violation in the cloud environment. Section 4 defines the method of data collection applied in this study. Section 5 provides perception into

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

organization through findings. Section 6 draws conclusions from the work conducted and presents recommendations and future work.

2. RELATED STUDIES

Weakness exploits wouldend in security breaches or violations of the architecture security policy causing data leakage or trust issues. Fevre et.al., (2012) studied that network administrators often give staff policies the benefits of doubt because employees don't always break the rules of malicious or vindictive reasons. Rather personnel may not even know that certain actions break company's policy. However, thousands of breaches occur daily and they cost companies million dollars. Breaches occurs when employees store organization information in third party cloud services or when they use a blacklisted app, jail broken phone or other devices that does not meet the organization guidelines.

Bardach et.al., (2015) guidelines for devices and software minimizes the way people really work and they won't need to go round restrictions. Educating staff on the risks of exposing company data increasesemployees' satisfaction, staff morale and convenience.

According to Kaufman (2009) most technological advances and regulators are typically in a "catch-up" mode to identify policy, governance, and law. To ensure that such decisions are informed and appropriate for the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods. To facilitate such policy and governance's emergence, the cloud providers threatens the entire cloud in which it resides.

There are six crucial areas in the cloud that require protection to be able to be adequate against the threats. These are Security of data at rest this means data should be secure when it is stored in the cloud servers. This is usually achieved by providing encryption for all data stored. Security of data in transit Means that data should be secure when being transferred from the cloud to the user computers. This can be achieved by providing TLS/SSL security. Authentication of users who have access to data should pass some sort of access control to be able to keep off unwanted users. These include strong passwords and biometrics among others.Robust isolation between data belonging to different customers although not applicable to private clouds, however for public clouds each customers data is isolated using different VMs.Cloud legal/regulatory issues where all customers should usually have their legal and regulatory experts inspect cloud provider policies and practices especially for things like data retention, deletion and security. Incident response this is where customers should understand how incidents and disasters would affect their data and should therefore implement relevant recovery procedures for the same (Felici & Pearson 2014).

3. CAUSES OF POLICY VIOLATION IN CLOUD ENVIRONMENT

3.1 Lack of policies and standards

One of the causes of policy violation is the lack policy and standards implementation by various organizations. Most of cloud users are not aware of the policies in place. Network administrators in various organizations have also not implemented and if they exist then they are weak policies (Pearson & Benameur, 2010).

3.2 Cloud computing security (or cloud security)

Cloud security is a subdomain of information security. Cloud security should address issues like protecting identity, maintaining privacy, and controlling access. It must also ensure that there is a business continuity and disaster recovery option with regular, continuous cloud backups in case of a breach or disaster. Lack of security, for instance, Hackers or unhappy customers could attack the cloud resources. There may be availability and reliability issues, insecure application programming interfaces, data loss/leakage, malicious insiders, and service and traffic hijacking, just to name a few sources of breaches (Kajiyama, 2013).

3.2.1 Malicious insiders: One of the benefits of cloud computing is that your organization doesn't need to know the technical details of how the services are delivered. The provider's procedures, physical access to systems, monitoring of employees, and compliance-related issues are transparent to the customer. Without full knowledge and control, your organization may be at risk (Saha et. al., 2014).

3.2.2 Data loss and leakage*:* With shared infrastructure resources, organizations should be concerned about the service provider's authentication systems that grant access to data. Organizations should also ask about encryption, data disposal procedures, and business continuity (Chen & Zhao, 2012).

3.3 Attacks on cloud

Another cause of policy violation is the attacks on the cloud. This can cause illegal access of confidential data in the cloud environment. This attack include theft of service attack

3.3.1 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 (Fangfei et.al., 2011).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

3.4 Legal and regulatory

Legal and regulatory issues are extremely important in cloud computing that have security implications. To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider's policies and practices to ensure their adequacy. The issues to be considered in this regard include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, trusted storage and trusted platform module access techniques can play a key role in limiting access to sensitive and critical data (Tianfield, 2012).

4. METHOD

Created on the rising industry interest in the cloud computing environment, it was imagined that current information security document are potentially putting organizations at risk. Therefore, this research critically assessed the causes of policy violation in a cloud environment through a survey and related literature on security policies on the cloud environment. The survey was sent out to 132 respondents' users on different organizations using cloud environment.

5. FINDINGS

The industry itself should establish coherent and effective policy and governance to identify and implement proper security methods. To facilitate such policy and governance's emergence, the cloud service providers threatens the entire cloud in which it resides.

The findings on the Causes of policy violation in the cloud environment is presented in table below about (37%, χ^2 =57.2, P≤0.0001) of the respondents strongly agreed that security policies in place safe guard their data in clouds. This was supported by (Rimal, 2009) who stated that cloud computing provides a storage facility that is hosted and accessible over the internet, making data readily available when and as required with security in place. Majority of respondents (79%, χ^2 =70.9, P≤0.0001) (strongly agreed and agreed) that lack of proper standards in place can affect their data in the clouds this claim was supported by (Mchugh, 2000).

The results of the respondents strongly disagreed (67%, χ^2 =33.1, P≤0.0001) that their information in the cloud environment has been attacked many times. There is only (6%) of the respondents who thought with lack of proper standards in place can affect their data in the cloud this was supported by (Quah, 2013). When respondents were asked whether they think their passwords are protected to ensure data is safe, (75%, χ^2 =62.1, P≤0.0001) (strongly agreed and agreed) that their passwords are protected to ensure data is safe. This claim was supported by 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.

The findings also stated that (35%, χ^2 =41.4, P≤0.0001) strongly agreed that data stored in cloud computing is private and confidential. Majority of respondents (strongly agreed and agreed) (45%, χ^2 =4.5, P≤0.0001) that applicable laws and regulations are weak there for non-compliance these claims were supported by (schulz, 2016).

	SD	D	UN	A	SA	χ^2	Pr> χ^2
Security policies in place safe guard my data in clouds	1.03	9.28	13.4	39.18	37.11	57.2	<.0001
Lack of proper standard in place can affect my data in the clouds	1.01	4.04	16.16	34.34	44.44	70.9	<.0001
My information in the cloud environment has been attacked many times	30.61	36.73	13.27	13.27	6.12	33.1	<.0001
My password is protected to ensure data is safe	3.03	5.05	17.17	29.29	45.45	62.1	<.0001
Data stored in cloud computing is private and confidential	2.02	13.13	15.15	34.34	35.35	41.4	<.0001
Applicable laws and regulations are weak there for non-compliance	11.46	20.83	22.92	22.92	21.88	4.5	<.0001

6. CONCLUSION AND FUTURE WORK

Cloud computing is still a new technology. This is an emerging technology which will bring about revolutions in terms of business models and applications. However, cloud computing faces challenges related to privacy and security, policy standards and regulations.

The global dimension of cloud computing requires standardized policy in each organization and practical solutions to enable stakeholders to assess their risks and establish adequate protection levels.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

RECOMMENDATIONS

Causes of policy violation should be communicated to users and penalties for violation should also be put in place to enable self-discipline. Standard policies should be strictly implemented in clouds and organizational/governing bodies should visit clouds' organization's infrastructure on regular bases to evaluate the efficiency of the security precautions adopted by the purveyors.

The government should have national cloud policy, laws and standardized SLA to prevent cloud clients from exploitation since CSP has an upper hand and secretion in implementing the SLA

REFERENCE

[1] Bardach, E., &Patashnik, E. M. (2015). *A practical guide for policy analysis: The eightfold path to more effective problem solving*. CQ press
[2] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.
[3] Fangfei Z., Goel M., Desnoyers P., Sundaram R., (2011). Scheduler vulnerabilities and coordinated attacks in cloud computing. In Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, pp. 25–27.
[4] Felici, M., & Pearson, S. (2014, June). Accountability for data governance in the cloud. In *Summer School on Accountability and Security in the Cloud* (pp. 3-42). Springer, Cham.
[5] Fevre, R., Lewis, D., Robinson, A., & Jones, T. (2012). INSIGHT INTO ILL-TREATMENT IN THE WORKPLACE: PATTERNS, CAUSES AND SOLUTIONS. *Contemporary Readings in Law & Social Justice*, *4*(2).
[6] Kajiyama, T. (2013). *Cloud computing security: how risks and threats are affecting cloud adoption decisions* (Doctoral dissertation, San Diego State University).
[7] Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy*, *7*(4).
[8] Kundra, V. (2011). Federal cloud computing strategy.
[9] Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 693-702). IEEE.
[10] Pearson, S., &Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 693-702). IEEE.
[11] Ramgovind, S., Eloff, M.M. and Smith, E. (2010) 'The management of security in cloud computing, School of computing, Universit of South Africa, Pretoria', *IEEE*, 2010.
[12] Rimal, B. P., Choi, E., &Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on* (pp. 44-51). Ieee
[13] Saha, T., Sen, P., & Datta, A. (2014). Security and Privacy Issues In Cloud Computing. *Communication, Cloud and Big Data: Proceedings of CCB 2014*.
[14] Tianfield, H. (2012, October). Security issues in cloud computing. In *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 1082-1089). IEEE.
[15] Zhang, Q., Cheng, L., &Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.