International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 8 Issue 4 April - 2024, Pages: 127-131

Information Security Governance in Cloud Computing

Najla S. Alsaikhan, Reem H. Algwinam, Salma Abdullah Alfohaid, Omer Alrwais

Najla S. Alsaikhan	Reem H. Algwinam	Salma Abdullah Alfohaid	Omer Alrwais
Dept of Information Systems	*Dept of Information Systems*	*Dept of Information Systems*	*Dept of Information Systems*
King Saud University	*King Saud University*	*King Saud University*	*King Saud University*
Riyadh, Saudi Arabia	Riyadh, Saudi Arabia	Riyadh, Saudi Arabia	Riyadh, Saudi Arabia
443920340@student.ksa.edu.sa	443920339@student.ksa.edu.sa	443920363@student.ksa.edu.sa	Oalrwais@ksu.edu.sa

Abstract*—The objective of this paper is to identify the impact of Information Security Governance (ISG) on reducing the risk of cloud computing, by discussing some of the essential points of cloud governance, like the leadership, organizational structures, and processes that safeguard information inside an organization. Most organization and company are migrating their data, software, and processes to the cloud and therefore it is critical that the cloud be governed by appropriate policies and procedures. Government agencies may resist moving their data to the cloud regarding confidentiality and the risk of leakage and much more. Accordingly, a case study of implementing cloud services in government agencies in Saudi Arabia and the differences in adopting the cloud India's e-governance cloud services.*

Keywords**—Information Security Governance, Cloud Com- puting, Security Governance Framework, Cloud Lifecycle.**

I. INTRODUCTION

By protecting people, processes, and technologies, cloud security governance is a control and management model aiming to optimize business computing in the cloud. Protocols and standards for cloud governance are intended to boost effectiveness, consistency, and organization.

A fundamental framework for corporate standards for cloud infrastructure and programming is also provided by cloud security governance. Because every cloud user has a unique operational structure, each organization or business must develop its governance model. For this reason, the architecture of cloud security governance is adaptable to the goals and needs of businesses.

A. Overview of Information Security in Cloud Computing

Implementing cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. Before adopting this technology, enterprises should analyze the company/organization's security risks, threats, and available countermeasures. Throughout the years, organizations have experienced and will continue to partake in this cloud computing era numerous system losses, which will directly impact their most asset and information, so its protection is of utmost importance to all organizations. The cloud computing rate will skyrocket and vulnerability to viruses, and cyberattacks will increase with many hacks. So, a lot of countries and companies over the world now working with a strong plan to prevent and minimize any future problems.[6]

B. Cloud Computing: Benefits, Risks, and Services for Information Security Governance.

The European Network and Information Security Agency (ENISA) published a guide that determined the risk to security and using cloud computing benefits. It also provides security guidance for the users. This guide reviews technical and legal risks for any big organization, by providing the loss of governance that stands out and reflects the loss of control when services are outsourced to a third party. Some of these risks are used as a starting point for the introduction of an information assurance framework, which is based on the controls from the ISO 27000 family. Not applying governance strategy and controls may make complying with the security governance requirements losses confidentiality availability and integrity of the entities data which leads to performance and quality issues of service.[7]

C. Cloud Services in The Market:

1) Amazon Web Service (AWS): the most popular cloud services provider on the market globally. AWS is a platform that provides many services and features from scratch to built-in technologies. Infrastructure is one of the services AWS provides and has a variety of technologies. For example, a variety of databases. Specifically, provide data lakes and data warehouses. Also, machine learning and many artificial intelligence supporting technologies that make the application built more effective and faster. In addition, AWS provides different tools that each client can choose the best match to their preferences. AWS claims that has comprehensive services and the most secure platform compared to other cloud providers.[1]

2) Microsoft Azure: is a cloud platform operated by Microsoft that provides all the cloud service types software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) to support business needs with a variety of tools and frameworks. [2]
3) Google Cloud Platform: offered by Google uses google core infrastructure, AI, and analytics tools. It also provides a security system that protects the data the same as the one google uses for its applications. Google uses pricing techniques for its cloud services based on the region the application runs on. It also has technical assessments from its technical team and many free products that users can use and improve their applications with. [3]
4) IBM Cloud Services: a platform that has a hybrid approach that supports public and private cloud services. It provides secured data and application infrastructure using edge-to-cloud protection. In addition, IBM Cloud provides popular and trustworthy AI tools that support business predictions. [4]

Also, there are much more cloud services providers such as Adobe creative cloud, Red Hat, VMware, Dropbox, and the Saudi governmental cloud "DEEM" which is recently launched by the Saudi Data and Artificial Intelligence Authority (SDAIA) to support the Saudi government agencies implementing cloud services with a secure and efficient infrastructure. [5]

II. ISG FRAMEWORKS

The scope of this review is limited, in a more practical manner, to a set of differentiating features suitable for the cloud computing area. Security aspects that are well known by some small business company communities and taken into account in most of the approaches are not dealt with in our comparison. The analysis shows that current ISG proposals show a lacks in matters such as value delivery through IT or control and accountability. Whenever a company decides to use cloud computing services, its managers need to make additional efforts regarding redefining the processes affected. Processes that have traditionally taken place in the company or even in a department are now controlled by the cloud provider. The creation of the audit and the control hold the additional security controls that should be established in the new cloud relationship. The Service Level Agreement (SLA) is a tool that permits customers to specify the security requirements they expect during the service provision and should offer a commitment to provide the security services required by the cloud provider. It includes a definition of new security controls, the specification of security metrics for evaluation, performance management by monitoring security strategies and processes, and tools that allow cloud provider logs to be accessed.[8][9][10]

III. CLOUD COMPUTING MODEL

Combining the SACS with the existing architecture of cloud computing, a security model of cloud computing is constituted, as shown in Fig.1

The process in the security model:

First, the user creates a local user agent and establishes a temporary safety certificate; then user agent uses this certificate for secure authentication in an adequate period—this certificate, including the host. name, user name, user ID, start

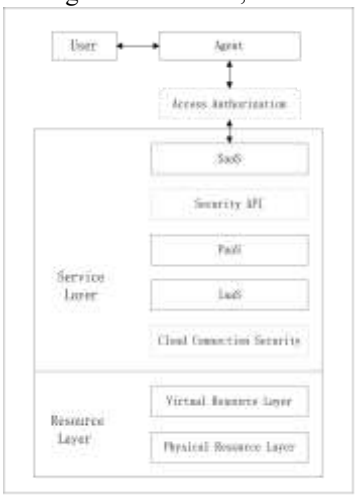

Fig. 1. Cloud Computing Model[11]

time, end time, and security attributes, etc., the user's security access and authorization are complete.

Second, when the user's task uses the resource on the cloud service layer, mutual authentication occurs between the user agent and specific application; while the application checks, if the certification for the user agent is expired, a change happened to the local security policy.

Third, according to the user's requirements, the cloud application will generate a list of service resources and then pass it to the user agent. Through security API, the user agent connects specific services. and cloud connection security ensures the safety of resources provided by the resource layer.

The security API in this model should be achieved with the SSL method, while the realization of cloud connection security uses SSL and VPN methods.[13]

Fig. 2. The system modules of SACS[12]

The concept of Security Access Control Service (SACS). Fig.2 represents the composition of its system modules. SACS includes access authorization, Security API, and cloud connection security. Access authorization is used to authorize users who want to request cloud service; security API keeps users using specific services safely after accessing the cloud; cloud connection security ensures that the safe resource of the upper service layer is provided by the bottom resource layer.

IV. SECURITY AND CONTROL IN THE CLOUD

Information security governance provides some policies in cloud computing like requiring a multi-layered and data-centric perimeter that protects information with relevant controls. Tests information with relevant controls. As a minimum, these should incorporate:

- Data encryption.
- Authentication.
- Privileges and access management controls.
- A firewall.
- Application security.
- Anti-virus software.
- Vulnerability of the management, to make sure the system is patching.

Making security effective is very important, making threat detection enabled and manageable and real-time response. Organizations must be prepared and have a plan in place for how they will manage such incidents, using analytics across the multi-cloud environment to detect threats, vulnerabilities, and configuration weaknesses.[12][13]

V. CASE STUDY

In this section, we will study implementing cloud services for a government agency in this section, we will study cloud services for a government agency in Saudi Arabia cloud computing revolution helps developing countries to implement their e-Governance services at a very low cost and provide better services to them like India. For Saudi, they will be based on the ministry of communications and information technology because all government or semi-government agen- cies need to follow policy as it's the first provider of services in the country. Saudi's cloud-first policy has a governance structure that ensures that the implementation of cloud services is defined. There are six roles in the cloud-first policy for implementation governance as shown in Fig.3.

Fig. 3. Governance structure for Cloud First Policy in KSA [14]

All six roles mentioned point out the big project of the national transformation that aims to develop the necessary infrastructure and create an environment that enables the public, private and non-profit sectors to achieve vision 2030. Achieving this goal cannot be accomplished until the government operations are proper and supporting digital transformations will enable the private sector to develop economic partnerships, and also build social development. The cloud itself is a virtualization of resources such as networks, applications, servers, and services that store data and allow on-demand access to users. Due to the many advantages of cloud computing-the government sector is also affected by some non-compliance issues such as not measuring correctly for resources need and efficiency at each entity. The one of strong points of the national transformation program in Saudi is provided cloud computing offers features like availability and scalability, reliability, fault- tolerance, and an environment to incorporate big data. Digital governance today is totally different than it was when the study of "Internet governance" coalesced in 1990. Digital Government Units (DGUs) have quickly appeared as a preferred solution for tackling the overcost and under-performing digital services and lagging digital transformation plaguing some government DGUs represent commonly the machinery of government phenomenon insofar as they all exist at the center of the state and adopt a shared orthodoxy, fevering agile, user-centric design, open-source technologies, pluralistic procurement, data-driven decisionmaking, horizontal 'platform-based solutions, and a 'deliveryfirst' ethos. [14]

A. Cloud-Based E-Governance in India

The government of India is transcending from the traditional modus operandi of governance towards technological involvement in the process of governance. Currently, the government of India is in the transition phase and seamlessly unleashing the power of ICT in governance (Kumar, P. et al. 2020). In India too, as of now, nearly every state government has its egovernance model. Currently, cloud computing is being widely used in e-governance. The features of cloud computing help eGovernance to perform their technologies with a cost-effective solution. These features can be distributed widely and increase the quality of the services for the users. The governance on cloud (G-cloud) is implemented and designed to be used in government services. It is not merely enough to set up egovernance models, but its awareness amongst the masses is equally important.[15]

B. Indian Government Initiative (GI Cloud – MeghRaj)

The government of India has embarked upon an ambitious initiative - "GI Cloud" which has been named as 'MeghRaj' India's 'Cloud-King' project initiated by the government of India from December 2013 to adopt cloud computing technologies. MeghRaj will be a bridge between various Indian government departments, different State government departments, citizens, and business enterprises using the internet, and mobile services. The aim is to reduce time, money,

and complexities in day-to-day official processes. On February 4, 2014, the former union Minister of Communi- cations and Information Technology, Kapil Sibal launched the national cloud under "MeghRaj" initiative. Some of the features of the national cloud included a self-service portal, multiple cloud solutions secured Virtual Private Network (VPN) access, and multi-location cloud-based on nodes that were set up across India in National Data Centers of National Informatics Centre (NIC).
[15]

Fig. 4. GI Cloud (MeghRaj) Architecture [15]

C. Cloud E-Governance Challenges

The initial challenge is the government is losing the management of information. This will be a giant issue as trust may be the first key for the adoption of cloud computing, and since information is kept within the cloud, the government must reassure all information protection users on a constant level if the info is kept domestically since they can control and recovery any needed information. Recently, our government has begun to utilize cloud computing architectures, platforms, and applications to deliver services and meet the requirements of its constituents.

D. Computing Performance

Cloud computing is an on-demand to calculate service and supports multitenancy; therefore, performance mustn't suffer over the acquisition of recent users.

VI. DISCUSSION

Now all activities in Saudi a n d Indian governments are converted to new technology to help citizens easily control and delivery their needs with best practices ways. They focused on cloud computing to provide resources with high- quality software and applications for both.

Furthermore, E-Governance also focused on improving the infrastructure at many levels specifically in higher senior workers and resources to increase security and reduce the cost. Since Saudi is willing to digitally transforming with very high quality and faster technologies. Indian e-Governance technology may be adapted to Saudi government applications to have efficient results that help on improving the current state. For further studies, other developed countries' cloud governance strategies may be revised to complete the gaps on both Saudi and Indian governance.

VII. CONCLUSION

In conclusion, governance's role in cloud computing is important. Making an efficient structure will impact the success of the implementation. The decision to move data into the cloud servers is no longer in the hands of the company. cloud computing is growing all over the world every day with new services and in the future development of cloud computing security. We suggest keeping the infrastructure environment under the latest update every time and using governance in intensified ways.

technologies, so it needs strong control and high security to prevent any attack that penetrates the government environment. The findings of this research will be helpful

VIII. REFERENCES

[1] "What is cloud computing? - aws.amazon.com." [Online]. Available: https://aws.amazon.com/what-is- cloud-computing/. [Accessed: 18-Nov-2022].

[2] hirenshah1 "What is Azure Cloud Services (classic)," What is Azure Cloud Services (classic) — Microsoft Learn. [Online]. Available: https://learn.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me. [Accessed: 18-Nov-2022].

[3] Google. [Online]. Available: ttps://cloud.google.com/. [Accessed: 18-Nov-2022].

[4] "IBM Cloud," IBM. [Online].Available: https://www.ibm.com/sa-en/cloud. [Accessed: 18-Nov-2022].]

[5] SDAIA)]SDAIA launches official identity of Governmental Cloud "deem" the official Saudi Press Agency. [Online]. Available: https://www.spa.gov.sa/2143627. [Accessed: 18-Nov-2022].]

[6] Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, A. et al. (2009, February). Above the clouds: A Berkeley View of cloud computing. Retrieved on March 10, .

[7] Bendandi, S. (2009). scribd.com. Cloud computing: Benefits, risks and recommendations for information security. Retrieved on March 15, 2010 from http://www.scribd.com/doc/23185511/Cloud-Computing-benefits-risks-and-recommendationsfor-information- security

[8] [Armbrust (2009)] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. "Above the Clouds: A Berkeley view of Cloud Computing", University of California, Berkeley (2009).

[9] [Bisong (2011)] Bisong, A. and Rahman, S. S. M. "An overview of the Security Concerns in Enterprise Cloud Computing." International Journal of Network Security Its Applications (IJNSA) 3(1): 30-45 (2011).

[10] [Bowen (2006)] Bowen, P, Hash, J. and Wilson, M. "Information Security Governance". Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology: 2-19 (2006).

[11] [Heiser J Nicolett M.Assessing the Security risks of cloud computing. http://www.gartner.com/DisplayDocument?id=685308,20 08

[12] Michael Airburst, Armando Fox, Rean Griffith, Above the cloud: A Berkeley View of Cloud Computing[R] Technical Report No.UCB/EECS-2009-28

[13] Heiser C.Kang, Z.WeiMing, Cloud computing: system Instance and Current Research, Journal of software, 2009.20(5):1337-1347

[14] "ةزازو تلااصتلاا ةينقتو تامولعملا." [Online]. Available: https://www.mcit.gov.sa/sites/default/files/ksa_cloud_first_policy_en.pdf.

[15] C. VijaY Assistant Professor, Department of Commerce St. Peter's Institute of Higher Education and Research, Chennai, Tamil Nadu, India "Cloud-Based E-Governance in India" http://orcid.org/0000-0003-0041-74