EFFECTIVE METHOD FOR MANAGING AUTOMATION AND MONITORING IN MULTI-CLOUD COMPUTING: PANACEA FOR MULTI-CLOUD SECURITY SNAGS

Uchechukwu Emejeamara[1], Udochukwu Nwoduh[2] and Andrew Madu[2]

[1]IEEE Computer Society, Connecticut Section, USA
[2]Department of Computer Science, Federal Polytechnic Nekede, Nigeria.

ABSTRACT

Multi-cloud is an advanced version of cloud computing that allows its users to utilize different cloud systems from several Cloud Service Providers (CSPs) remotely. Although it is a very efficient computing facility, threat detection, data protection, and vendor lock-in are the major security drawbacks of this infrastructure. These factors act as a catalyst in promoting serious cyber-crimes of the virtual world. Privacy and safety issues of a multi-cloud environment have been overviewed in this research paper. The objective of this research is to analyze some logical automation and monitoring provisions, such as monitoring Cyber-physical Systems (CPS), home automation, automation in Big Data Infrastructure (BDI), Disaster Recovery (DR), and secret protection. The Results of this research investigation indicate that it is possible to avoid security snags of a multi-cloud interface by adopting these scientific solutions methodically.

KEYWORDS

Multi-Cloud, CSP, Vendor Lock-in, Cyber-crime & BDI.

1. INTRODUCTION

Cloud computing refers to a virtual platform where users are permitted to handle necessary computational facilities, namely, servers, applications, storage spaces, and networks, remotely. CSPs generally offer cloud computing facilities that can be accessed from different types of interfaces such as desktops, laptops, tablets, and smartphones. Widespread demands (as can be reflected from Table 1) of cloud computing in both personal and professional sectors have prompted the researchers to concentrate sincerely on this topic. As a result, the next version of cloud computing, in particular multi-cloud computing, has got its entrance in the virtual world. Multi-cloud systems are allowed to utilize various cloud platforms from numerous CSPs in storing, sharing, or analyzing data files. Schematic views of single and multi-cloud environments are shown in Figure 1 and Figure 2 respectively. Although multi-cloud is a highly efficient and popular computing technology, appropriate security is still a concerning issue of this service. One of the main reasons for this drawback is the homomorphic encryption of a multi-cloud mechanism [1]. Intensive research investigations are going on to address security-related inefficiencies of a multi-cloud platform. Intellectual automation management and logical monitoring may be regarded as fruitful solutions in resolving these disadvantages of multi-cloud and introducing its upgraded version in the near future.

Table 1. Worldwide cloud infrastructure spending and annual growth (Reproduced from https://www.parkmycloud.com/blog/aws-vs-azure-vs-google-cloud-market-share/)

Cloud Service Provider	Q4 2019 (US billion)	Q4 2019 market share	Q4 2018 (US billion)	Q4 2018 market share	Annual growth
AWS	9.8	32.4%	7.3	33.4%	33.2%
Microsoft Azure	5.3	17.6%	3.3	14.9%	62.3%
Google Cloud	1.8	6.0%	1.1	4.9%	67.6%
Alibaba Cloud	1.6	5.4%	1.0	4.4%	71.1%
Others	11.6	38.5%	9.3	42.4%	24.4%
Total	30.2	100%	22.0	100%	37.2%

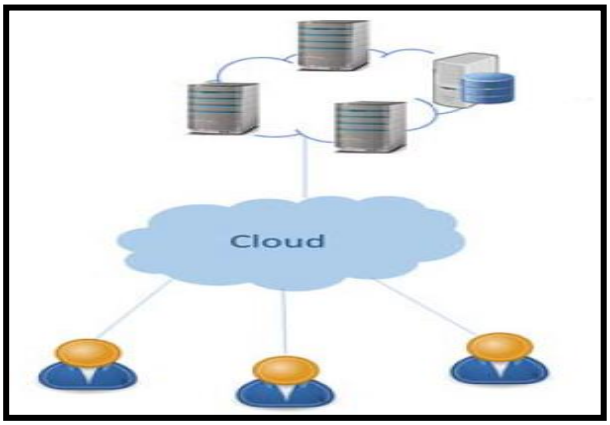

Figure 1. Single cloud infrastructure [8]

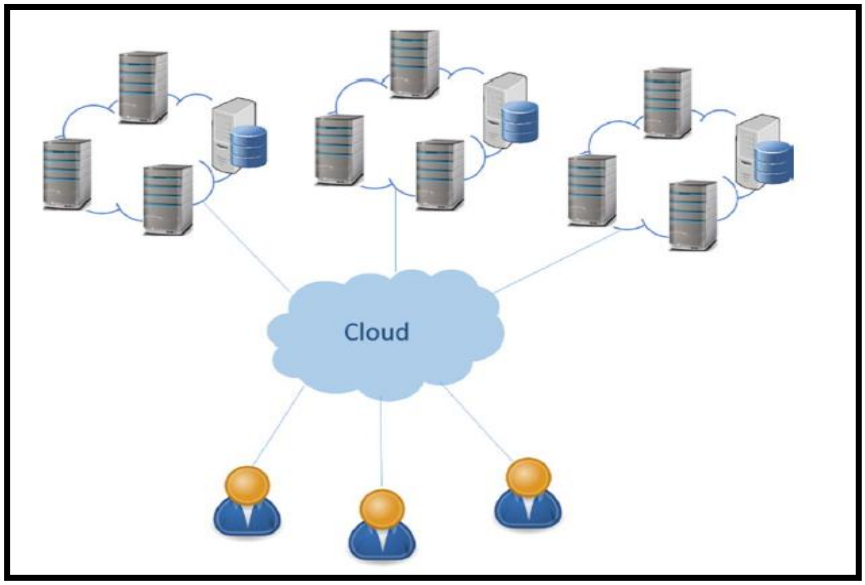

Figure 2. Multi-cloud infrastructure [8]

2. SECURITY SNAGS IN MULTI-CLOUD COMPUTING

It is mentioned in the above section that data protection is a serious problem in multi-cloud systems. Therefore, it is essential to discuss the main challenges of this service briefly before concentrating on the solution methods.

2.1 Threat Detection and Incident Response

Hacking and cyber-attacks are well-known difficulties with any type of cloud computing. Implementations of proper threat detection and Incident Response (IR) tools can resolve this problem. According to [2], this complication is predominant in multi-cloud due to inadequate numbers of detective controls, such as Intrusion Detection Systems (IDS) and firewalls. Ensuring timely threat detection remains as a challenge for both CSPs as well as the users of this service.

2.2 Data Protection

Secure protection of confidential documents is one of the most important factors in storing data in the virtual world and avoiding unwanted data loss. Colombo et al. have manifested that it is challenging to offer guaranteed data protection in a multi-cloud because Virtual Machines (VM) of each of the cloud platforms are different [3]. It is not easy to synchronize them using encryption and decryption. Also, dissimilarities between the types of storage spaces of the different clouds of a multi-cloud system are another reason for this inefficiency.

2.3 Situation of Vendor Lock-in

Another threat with a multi-cloud interface is the circumstances of vendor lock-in, which is defined as a state where the client becomes dependent on the network service provider. This situation reduces the client's flexibility in changing CSP or transferring data from one CSP to another. Complexities include huge data transfer costs, legal questions, and technical incompatibilities [1]. This problem is severe in the case of multi-cloud platforms because of the large number of connected CSPs in a single system. Authorized customers can easily access confidential documents at any time and from any place or vendor, which allows cloud brokers in performing cyber-crimes such as attacking, hacking, and sharing important data files [4]. In this way, brokerage threats are predominant in a collaborative multi-cloud interface and scientific intervention of this problem is necessary.

3. AUTOMATION AND MONITORING TECHNIQUES

Renowned scientists around the globe are continuously conducting sincere research investigations to prevent security snags of a multi-cloud interface. Proper monitoring with the provision of automation has been identified as an effective way-out in this context. Some of these techniques have been explored in the following paragraphs concisely.

3.1 Monitoring of Cyber-Physical Systems

CPS is a framework that combines computers and networks with physical procedures. Acute monitoring of CPS in a multi-cloud environment is required in providing hazard-free computational facilities. Noor et al. have proposed a modern infrastructure, namely, Multi-cloud Monitoring in Cyber-Physical Applications (M2CPA) in this regard [5]. An outline of this architecture is depicted in Figure 3. Monitoring managers and monitoring agents (symbolized by Ã) are the main components of this technique. A manager is responsible for monitoring the performances (data analysis, storage, and threat prediction) of multiple VMs of its region.

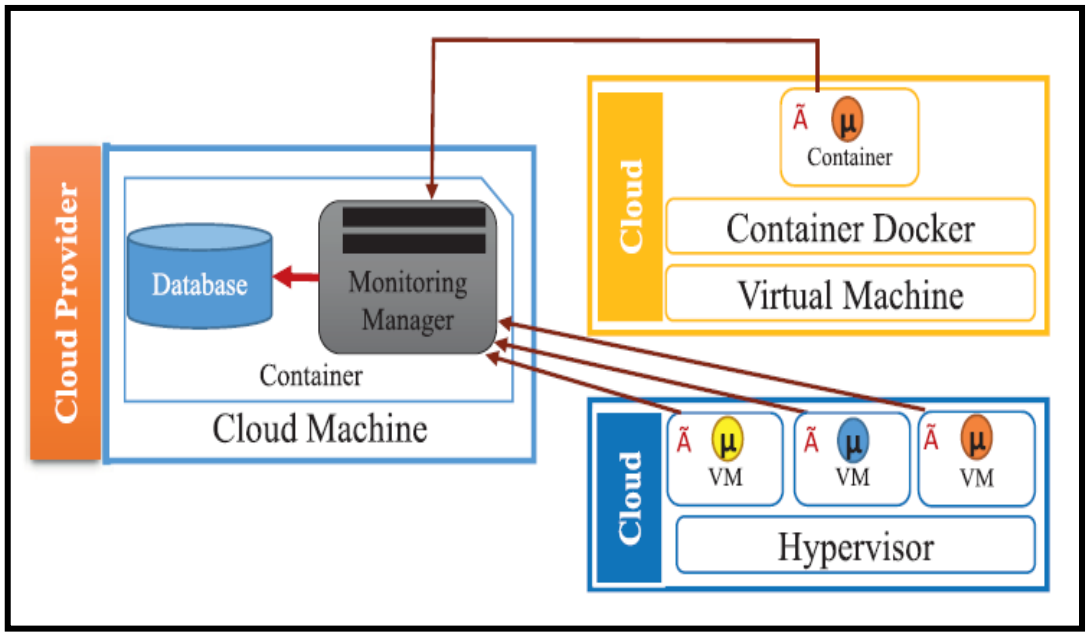

Figure 3. Outline of M2CPA architecture [5]

3.2 Smart Home Automation

Home automation is a facility that ensures users in managing multi-cloud computations with greater security. Shankar et al. have initiated a home-based automation solution by using low energy and cheap Integrated Circuits (IC), and the universal Google Cloud Platform [6]. Along with this, they have associated the Internet of Things (IoT) with this technology that offers clients to monitor and control data in multi-cloud smartly as well as safely.

3.3 Automation in Big Data Infrastructure

BDI is one of the main components of a multi-cloud system. Privacy issues are vital in monitoring large amounts of data files. SlipStream cloud automation is an efficient method in this context [7]. It is an open-source virtual application framework that promotes automated multi-cloud management skilfully.

3.4 Disaster Recovery

Recovery of data files after any disaster (natural or man-made) can be considered as an important security issue in multi-cloud, as it generally consists of huge amount of documents. Alshammari

et al. have manifested that guaranteed DR is possible in multi-cloud by creating at least three duplicates of all data files in the same cloud location or more preferably three different virtual locations [8]. Nevertheless, the main obstacle in implementing this technique is the fact that such a data backup procedure is expensive and requires a large amount of storage capacity.

3.5 Secret Protection in Public Multi-Cloud Access

Security of secret documents in public cloud computing services (for example, Amazon, Microsoft, and Google) is required to maintain the trustworthiness of the providers and offering users cost-effective but safe cloud computation. Remarkably, this necessity is more demanded in multi-cloud access [9]. Data protection layers in the multi-cloud technique are showed in Figure 4. It can be inferred from this figure that a secret data can be protected by three layers, namely, Compressed Data, Digital Signature, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Ciphertext. On the other hand, sharing of a secret data may also be secured by two stages: Share Hash Message Authentication Codes (HMACs) and Cloud Data Stores (CDS) Encryption.

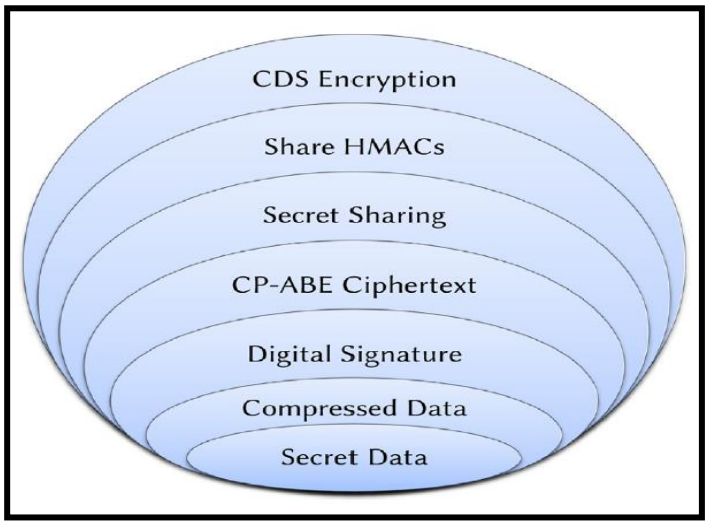

Figure 4. Secret sharing framework [9].

4. CONCLUSIONS

Through the thorough analysis of the security concerns of multi-cloud technology and their logical interventions, threat detection and IR, data protection, and vendor lock-in have been identified as the three main security drawbacks of this interface. Several types of automation and monitoring suggestions have been explored in dealing with these inefficiencies. Some of them are M2CPA, smart home automation, SlipStream automation in controlling BDI, DR, and secret protection. It can be expected that they will help provide scientific solutions to the security snags of a multi-cloud environment and may reduce the probability of future cyber-crimes precisely.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] J. Hong, T. Dreibholz, J. A. Schenkel, & J. A. Hu, "An overview of multi-cloud computing," in *Web, Artificial Intelligence and Network Applications*, vol. 927. Cham, Switzerland: Springer, 2019, pp. 1055-1068, Mar. 2019, doi: 10.1007/978-3-030-15035-8_103.

[2] K. A. Torkura, M. I.H. Sukmana, F. Cheng, & C. Meinel, "SlingShot-Automated threat detection and incident response in multi cloud storage systems," *Proc. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA) Conf.* Cambridge, MA, USA, 2019, pp. 1-5, doi: 10.1109/NCA.2019.8935040.

[3] M. Colombo, R. Asal, Q. Hieu, F. A. El-Moussa, A. Sajjad, & T. Dimitrakos, "Data protection as a service in the multi-cloud environment," *Proc. 2019 IEEE 12th International Conference on Cloud Computing (CLOUD) Conf.* Milan, Italy, 2019, pp. 81-85, doi: 10.1109/CLOUD.2019.00025.

[4] B. Aldawsari, T. Baker, M. Asim, Z. Maamar, D. Al-Jumeily, & M. Alkhafajiy, "A survey of resource management challenges in multi-cloud environment: Taxonomy and empirical analysis," *Azerbaijan Journal of High Performance Computing*, vol. 1, no.1, pp. 51-65, July 2018, doi: 10.32010/26166127.2018.1.1.51.65.

[5] A. Noor et al. "Cyber-physical application monitoring across multiple clouds," *Computers and Electrical Engineering*, vol. 77, pp. 314-324, July 2019, doi: 10.1016/j.compeleceng.2019.06.007.

[6] V. R. Shankar, S. Suchitra, B. Pavithra, P. S. Rajendran, S. G. G. Sophia, & M. J. Leo, "Energy optimization for smart home automation in multi-cloud environment," *Proc. 2020 International Conference on Inventive Computation Technologies (ICICT) Conf.* Coimbatore, Tamil Nadu, India, 2020, pp. 534-539, doi: 10.1109/ICICT48043.2020.9112537.

[7] Y. Demchenko, F. Turkmen, C. de Laat, C. Blanchet, & C. Loomis, "Cloud based big data infrastructure: Architectural components and automated provisioning," *Proc. 2016 International Conference on High Performance Computing & Simulation (HPCS) Conf.* Innsbruck, Tyrol, Austria, 2016, pp. 628-636, doi: 10.1109/HPCSim.2016.7568394.

[8] M. M. Alshammari, A. A. Alwan, A. Nordin, & I. F. Al-Shaikhli, "Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges," *Proc. 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS) Conf.* Salmabad, Iran, 2017, pp. 1-7, doi: 10.1109/ICETAS.2017.8277868.

[9] P. Junghanns, B. Fabian, & T. Ermakova, "Engineering of secure multi-cloud storage," *Computers in Industry*, vol. 83, pp. 108-120, Dec. 2016, doi: 10.1016/j.compind.2016.09.001.