IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 32-34
www.iosrjournals.org

Security Alliance Framework based on Machine Learning to Develop Cloud

M. M. Syed Sulaiman *Research Scholar,*
Department of Computer Science,
Quaid-E-Milleth Govt college for women,
Chennai.

Dr. K. Nirmala, *Associate professor,*
Department of Computer Science,
Quaid-E-Milleth Govt college for women
Chennai.

Abstract:
The number of customers looking for a cloud service station that will guarantee the privacy and protection of their data is now on the rise. Multi-cloud solutions, which provide the chance to enhance data security while likewise lowering the expense of software development, have started to be integrated into a variety of exciting application domains in order to achieve this purpose. This new development is exciting. It is a difficult problem to solve, but it might be difficult to determine the best method for distributing a cloud application's components among resources offered by several providers. Each service provider has specific performance and protection requirements that must be met. This paper provides ain-depth approach for maintenance.
Keywords*: Security Alliance, Machine Learning, Cloud Security*

I. Introduction

In recent years we have seen the rise of new methodologies and technologies that make it easier to produce cutting-edge information and communication technology solutions and automate their implementation. This was one of the most exciting improvements in this field [1]. The growing interest in adopting multi-cloud techniques to improve business performance while reducing costs and increasing security levels is an indication of this trend. Consuming the services of different CSPs that are not affiliated with a federation is called multi-cloud, and multi-cloud is used to describe this activity. [2] The term multi-cloud is also used to describe the behaviour itself. If you have more than one type of infrastructure, you can serve a greater variety of consumers. This is because you have more options to choose from. It also reduces the risk of your data being corrupted or your service is interrupted due to a single point of failure as a direct result of your actions. In addition, it may be of interest to distribute the components of an application via the service providers that offer the best possible level of security assurance according to the application's requirements. This can be advantageous for several reasons [3].

If we can keep up with the increase in internet usage that has taken place worldwide [4], we will need heavy-duty tools for managing data stored in the cloud. The need for cloud computing has spread beyond information technology to other industries, leading to the emergence of new business opportunities. Cloud computing can now be used in a wider variety of contexts. Computing in the cloud has experienced a spectacular surge in reputation in recent years and is currently one of the technologies used by most people [5]. In the field of recent computer science, cloud computing is one of the topics that receives the most attention and discussion. The fields of information technology, economics, software development and data storage were all significantly influenced by his debut. The primary goal of cloud computing is to provide services to customers while reducing the financial burden associated with associated equipment and software. These services offer a distributed building capable of performing high levels of processing, in addition to a system for storing data online that is secure, fast and well-suited to the activity at hand. The cloud gives users access to a multiplicity of on-demand service alternatives that are not only convenient but also customizable [6].

The cloud not only fulfils users' hardware requirements and the software and data stored on cloud servers by those users, but also keeps in touch with new technologies and provides a common platform to meet user expectations [7 -8th]. Customers have absolutely benefited from the ubiquitous availability of cloud computing as well as the ease of use of the services provided. Despite this, the technology still faces a number of significant experiments, including privacy and legal issues. It is necessary to establish security protocols for every component of the cloud architecture, including network, host, application and data storage. This must be done. It is important to have a solid understanding of the potential dangers associated with cloud computing before committing to it long-term [9].

The vulnerabilities that already exist in a system or organization become an even greater risk as the use of new technologies becomes more widespread. When faced with a larger threat, an additional risk factor must be considered: susceptibility. At the same time, advances in security technology are being made to build

countermeasures for intrusions carried out by hostile parties. Many factors are considered when classifying vulnerabilities, including the type of attack, how that attack interacts with the system, and the attacker's goals [10].

Although multi-clouds hold great promise, there are still a number of partial questions about them [11]. Even if there is only one provider, the issue of security can become more complicated as different CSPs have implemented different security standards and laws. When many different cloud service providers work together to offer a single application, the complexity of the scenario increases significantly. In addition, it depends on the way the application components communicate with each other and how this affects the implemented security policies [12]. It also depends on the way the application components communicate with each other. As a result, choosing an appropriate configuration for deployment becomes much more difficult: there are an inordinate number of aspects to consider before a developer can decide how to effectively partition application parts between different vendors, each with their own unique service level agreements and transport mechanisms [13].

II. Related Works

This study contributes to the development of the profession in several ways, one of which is the formalization of the difficulties of use. This topic has been the focus of numerous studies, the vast majority of which use techniques originally developed for use in other contexts. In the beginning, these techniques were used to perform calculations on different grids and clusters. It was only much later that they were modified to work properly with clouds [16].

The non-functional requirements for cloud-based apps are mostly communicated informally. For example, considerations such as cost, performance, scalability, and similar considerations may play a role in deciding which configuration and deployment options are ultimately chosen. Other considerations such as these may also be relevant. Because of the way these various components interrelate with each other, finding the optimal solution is not an easy task. This article [17] focuses on safety as this is the only non-functional requirement for the study. Security is widely recognized as the single biggest downside to cloud computing, and this article explores that perception. If you are looking for literature related to our work, we encourage you to read it. It provides a multi-criteria optimization technique, also based on AHP, to identify the most viable architectural paths for cloud-based application deployment, with a focus on non-functional requirements. This strategy takes a number of different reasons into account.

The authors in [18] assumed that individual VM instances each have their own defining characteristics. Large performance differences between instances that are otherwise identical can be the result of a variety of causes, including but not limited to underlying hardware mismatches, conflicts, and other phenomena. These causes can also be the result of a combination of these and other factors. These variables may also contribute to the observed performance differences. They developed a formal model for placement methods that allowed them to experiment with a variety of alternatives before choosing the one that worked best for them.

The authors in [19], dedicated to exploring resource management, examine multi-tenancy challenges such as scalability and shared resources for the purpose of scheduling compute-intensive workflow applications. One of these problems is the scheduling of workflow programs that support multiple tenants. The policies for managing resources and the controls required to put those policies into action are two distinct respects addressed by this framework.

Forecasting the costs associated with deploying apps in the cloud required to meet Service Level Agreements (SLAs) based on performance is the objective in [20], which can be found here. It then automatically distributes the entire system across as few machines as possible, taking into account the components that are accessible, the requirements for those components, and the maximum number of virtual resources that can be used.

It is possible to use a distributed heuristic strategy like the one described in [21] to help the process of optimizing the deployment method. Because of the algorithmic architecture used by the technology, it is possible to reduce the amount of time and energy expended on the execution or communication between the different components of an application. This is made possible as a direct consequence of the use of the method.

III. Conclusions

This paper shows that there is an urgent need to protect the data now stored in the cloud. Cloud service providers use all available resources to ensure the privacy of their consumers' data. Nevertheless, the diverse security risks connected with cloud computing are the focus of this study. This section also contains a full explanation of the difficult conditions and potential security concerns associated with cloud computing, which are provided for your perusal. According to the results of the investigation, the preventive mechanism consists of a secured framework equipped with a system for conducting internal audits. This is done to better deal with threats coming from both inside and outside the party.

References

[1]. Kumar, R., &Goyal, R. (2021). Top threats to cloud: a three-dimensional model of cloud security assurance. In Computer Networks and Inventive Communication Technologies (pp. 683-705). Springer, Singapore.

[2]. Zhao, T., Gasiba, T. E., Lechner, U., & Pinto-Albuquerque, M. (2021). Exploring a Board Game to Improve Cloud Security Training in Industry (Short Paper). In Second International Computer Programming Education Conference (ICPEC 2021). SchlossDagstuhl-Leibniz-ZentrumfürInformatik.

[3]. Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. Computers & Electrical Engineering, 96, 107527.

[4]. Shaikh, N. S., Yasin, A., & Fatima, R. (2022). Ontologies as Building Blocks of Cloud Security. International Journal of Information Technology and Computer Science (IJITCS), 14(3), 52-61.

[5]. Sangui, S., & Ghosh, S. K. (2021). Cloud Security Using Honeypot Network and Blockchain: A Review. Machine Learning Techniques and Analytics for Cloud Security, 213-237.

[6]. Mohanty, S. N., Potluri, S., Prakash, V. B., Srinath, B., &Manjunath, B. (2021). Cloud Security Concepts Threats and Solutions: Artificial Intelligence Based Approach. Cloud Security: Techniques and Applications, 1, 1.

[7]. Shaikh, A. H., &Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking (pp. 63-77). Springer, Singapore.

[8]. Orue-Echevarria, L., Garcia, J. L., Banse, C., & Alonso, J. (2021). MEDINA: Improving Cloud Services trustworthiness through continuous audit-based certification. In CEUR Workshop Proceedings. CEUR-WS.

[9]. Shrmali, D., & Sharma, S. (2022). Applications of Deep Learning in Cloud Security. Deep Learning Approaches to Cloud Security, 225-256.

[10]. Anusha Linda Kostka, J. E., &Vinila Jinny, S. (2021). Data Security and Privacy Protection in Cloud Computing: A Review. Intelligence in Big Data Technologies—Beyond the Hype, 253-257.

[11]. Iosif, A. C., Gasiba, T. E., Zhao, T., Lechner, U., & Pinto-Albuquerque, M. (2021, December). A Large-Scale Study on the Security Vulnerabilities of Cloud Deployments. In Inernational Conference on Ubiquitous Security (pp. 171-188). Springer, Singapore.

[12]. Arivazhagan, N., Somasundaram, K., VijendraBabu, D., GomathyNayagam, M., Bommi, R. M., Mohammad, G. B., ... &PrabhuSundramurthy, V. (2022). Cloud-internet of health things (IOHT) task scheduling using hybrid moth flame optimization with deep neural network algorithm for E healthcare systems. Scientific Programming, 2022.

[13]. Gasimov, V. A., &Aliyeva, S. K. (2021, June). Using blockchain technology to ensure security in the cloud and IoT environment. In 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-5). IEEE.

[14]. Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2021). Raising awareness about cloud security in industry through a board game. Information, 12(11), 482.

[15]. Kousik, N. V., Jayasri, S., Daniel, A., &Rajakumar, P. (2019). A survey on various load balancing algorithm to improve the task scheduling in cloud computing environment. J Adv Res Dyn Control Syst, 11(08), 23972406.

[16]. Ometov, A., Molua, O. L., Komarov, M., &Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. Sensors, 22(3), 927.

[17]. Ometov, A., Molua, O. L., Komarov, M., &Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. Sensors, 22(3), 927.

[18]. Raja, R. A., Karthikeyan, T., &Kousik, N. V. (2020). Improved privacy preservation framework for cloudbased internet of things. In Internet of Things (pp. 165-174). CRC Press.

[19]. Saxena, S., &Nisha, T. N. (2021, July). Augmentation of SECaaS model with eCISO in cloud-based security services: A Comprehensive study. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042013). IOP Publishing.

[20]. Natarajan, Y., Kannan, S., &Dhiman, G. (2022). Task scheduling in cloud using aco. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 15(3), 348-353.

[21]. Jayachandran, R. (2021). A Feasible Review on Cloud Computing Security Services with Recent technologies used in the Digital Channels. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2340-2344.