JCST Journal of Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7642723

IMPLEMENTATION OF ADAPTIVE CLOUD SECURITY FRAMEWORK FOR CLOUD COMPUTING MONITORING SYSTEM APPLICATIONS

Kadapa Suneel Kumar and Dr. Nisarg Gandhewar
Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam University, Indore (M.P.) - 452010, India
Corresponding Author Email : sunilkumar1219@gmail.com

Abstract:
Various organizations implement cloud computing to store a significant amount of data in the clouds. Therefore, it may be necessary to secure data that may also be in the form of text, audio, video, and many other types. There are a number of algorithms created with the help of employing the researchers' methods for protecting the information in the cloud. In this paper implementation of Adaptive cloud security framework for cloud computing monitoring system applications. Cloud security has emerged as one of the most crucial challenges in cloud computing as a result of the industry's continued expansion. For instance, it is challenging to ensure the security of data hosted on a cloud platform since such data may be attacked. As a result, we must give consideration to the problem of how to safeguard data stored on the cloud. Data monitoring is a vital step in order to secure data. We create an autonomic computing-based cloud data monitoring system on the cloud platform, checking to see whether the data is out of the ordinary throughout the cycle and reviewing the security of the data in light of the results. In this paper, the feasibility of the scheme can be verified through simulation. The findings demonstrate that the suggested technique can properly assess the level of anomalous data and can adjust to the dynamic change in cloud platform load. Meanwhile, it increases the precision and timeliness of monitoring by automatically altering monitoring frequency. Additionally, it can lower the system's monitoring costs during routine operation.

Keywords: Cloud Computing, Cloud Security, Cloud Threats, Cloud Vulnerabilities, Data Security.

I. INTRODUCTION

With no management work or service provider participation, cloud computing is a concept that enables simple, on-demand network access to a shared pool of reconfigurable computing resources, such as networks, servers, storage, and applications. A distributed architecture known as cloud computing centralises the system's funding in order to offer computer resources and facilities on demand. Cloud platforms are offered by cloud service providers (CSPs) for their services. Similar to how Internet service providers supply high-speed customers' Broadband for Internet access, customers must utilise and develop their own online services. ISPs (Internet service providers) and CSPs both offer services. Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) are the three types of services that cloud providers often offer (IaaS). Since it was only necessary to pay for the services on the basis of usage, there are many reasons why businesses must use cloud storage. Organizations may successfully answer the demands of fast changing markets through comparative research, ensuring that they remain at the forefront [1].

Resource management of the cloud computing platform includes resource monitoring as a key component. It serves as the foundation for work scheduling, resource allocation, and load balancing. Users' expectations for cloud computing security have grown as a result of the widespread use of these services. It is hard for a typical security programme to protect the data security in the cloud platform due to the transparent virtualization and resource flexibility of the cloud computing environment, which limits the usage and development of cloud computing [2].

Therefore, it is crucial to create new technologies that are appropriate for monitoring data on cloud platforms. However, a big amount of monitored data will require a lot of resources to gather, transmit, store, and analyse, which will negatively impact system performance, early detection of abnormalities, and problem-solving precision. Additionally, because cloud computing is mostly based on current technology, any security flaws that exist will be instantly transferred to the cloud computing platform, thus posing a higher security concern.

Basically in cloud computing environment users lost their data and faces various security issues. To overcome this security issues encryption and decryption techniques are implemented to secure the data [2]. These techniques will help to recover the data when lost and secure the data from various attacks. This will mainly provide data confidentiality, data integrity. Account recovery, data recovery process in cloud computing environment helps to do more research by using different techniques. In distributed or grid systems, it plays a crucial role. However, there will be certain drawbacks if the aforementioned techniques are used directly in the cloud computing environment. On the other hand, the resource is highly virtualized and adaptable in the cloud computing environment. Different services are utilized in the cloud computing monitoring system like IaaS, SaaS and PaaS [3].

Users are required to monitor the virtual computer it is running. The customer will, however, be paid for consumption as such by the cloud service provider because cloud computing is a business model. Since the existing resource monitoring system's monitoring data does not have fine granularity, it is not possible to obtain process-level information or to see real-time resource utilization as user tasks are being carried out. The environment for cloud computing is open, disorderly, unexpected, and dynamic. Since cloud providers must charge users for relevant fees based on resource consumption, but the cloud computing environment will not meet the demands of original resource monitoring solutions.

Because of distributed cloud computing strategy different resource monitoring techniques are developed which are not fully adapted. Data monitoring strategy is implemented based on the automation which consists of different data mining models. The mechanism of automation is applied in cloud computing monitoring system to protect the data from the cloud platform [4].

The model is primarily made up of four modules: knowledge base, network monitoring, data analysis, reaction plan, and system implementation. The system collects the data stream and creates the original data in the network monitoring module. Additionally, the original data are prepared via the data preparation technique. The reaction strategy module adjusts the monitoring period based on the analysis result that the data analysis module provides after evaluating these processed data and extracting valuable data to decide if they are abnormal. The fundamental components of this paradigm, which give customers crucial data monitoring information, are data gathering and storage analysis [5].

II. LITERATURE SURVEY

First, taking 2011 into account, writers gave some information on cloud computing services and products including networks, storage, servers, services, and apps without really receiving them. According to the paper's observations, it has been noted that the overhead of the giant machine has decreased in terms of risk, information leakage, and so forth [6]. On-demand internet services are offered through cloud computing. If a company that offers internet services needs to invest a lot of money in infrastructure and problems like disc failure, system failure, and software defects, among other things. For those who no longer wish to build up infrastructure on personal devices, the cloud is a perfect answer.

[7] In accordance with this research, cloud users prefer to pay as they use services rather than investing money in infrastructure. In the year 2012, authors discussed cloud security, pointing out that while data is growing exponentially, the security of open-ended and easily accessible property is still debatable. They also looked into security risks associated with cloud computing environments, trends, cloud transport models, and cloud stakeholder. The authors just briefly touched on cloud protection. Since more people are using clouds to store, send, and retrieve sensitive information in recent years, cloud community protection has become one of the most pressing issues [8]. In the above artwork, the designer communicates some of these issues. Information corruption, main-middle attack, and privacy violation are risk issues that have an influence on cloud security. Because of its flexibility, cost effectiveness, and ability to convert data between clients and servers, the cloud is one of the most technologically advanced research environments.

[9] This article goes into detail to ensure that the transaction desk that includes the data is held while also managing the strong data security with the use of a recognition control device. Virtualization is crucial for cloud computing, but its safety hasn't been well investigated. This paper's analysis of cloud security focuses on how virtualization attacks affect good cloud computing issuer models. With the use of virtualization, cloud computing provides a platform for the exchange of assets that include software and infrastructure.

Which discuss cloud environment makes an effort to be trustworthy and adaptable while providing services. Cloud protection offers many protection patterns that cloud provider companies must adhere to. Cloud information is encrypted using the RSA set of standards and digital signatures. While data is being sent over a network, [10] defines the safety control models, protection requirements, and RSA set of rules with digital signature to increase cloud data security. It is shown that using several cloud providers to manage security has received a lot less attention from the research network in 2013 than using a single cloud provider. Finding many clouds, reducing safety risks, and information security are the main goals of this research. Motivations of cloud users loss of control on the part of the owner owing to data being moved away from organizational barriers and given access over the internet.

[11] Providing a brief summary of data security and maintaining a level of consensus among data owners has become crucial for cloud service providers. In addition to physical attacks, bad people have the possibility of harming sensitive data about people online. To prevent online attacks, you must take time to secure your company, personal information, and your country [12].

Data mining and algorithms play a particularly important role in this paper's mention of ensuring the security of cloud records. Internet of Things (IoT) and cloud computing are the most important tactics in our world in 2014. They will likely continue to be leased and used, which will make them the most important component of the net. [13] express interest in cloud computing and IoT integration, which is included as Cloud IoT. Since most businesses are moving their data to the cloud, it's critical to ensure the security and integrity of cloud users' data [14]. The cloud provides virtual pools of resources to cloud customers as a service via an internet interface. Cloud sources include infrastructure, community, platform, software programme, and storage.

The rapid growth of cloud computing also brings with it an increase in server security issues. It is difficult to track security threats, but one of the greatest ones is the Distributed Denial-of-Service (DDOS) attack, which is one of the best types of network intrusion in a cloud computing environment. [15] These attacks are presenting a way to identify and remove essential information.

III. ADAPTIVE CLOUD SECURITY FRAMEWORK

The below figure (1) shows the framework of adaptive cloud security system. In order to address the issue of cloud system security, we created a separate monitoring model based on the notion of autonomous computing. The five primary components of the model are the knowledge base, the response strategy, the system implementation, the network monitoring, and the data analysis modules. Traditional resource monitoring in the cloud computing context is possible in two different ways. (1) Active mode; the work node contains a resource monitoring component, and a virtual machine monitor gathers status data on the virtual machine it is hosting. The monitor transmits its own monitoring data in order to activate the master node. (2) In passive mode, the main node requests the work node to do a task, and the work node responds by sending the main node its monitoring data.

Network monitoring module is nothing but the combination of virtual machine, primary resources and other elements which help monitoring agent to install easily. Based on all levels the data is stored permanently without any fail. To access the data at correlation level data analysis module is established. By using the PCA (Principal Component Analysis), linear regression equation is assessed and computed statistically in cloud computing environment system. Based on the following steps monitoring of data is performed in the response strategy. By using the process of adaptive cloud monitoring system data is monitored step by step interval. The monitoring agent will be used by the system implementation module to carry out the dynamic adjustment of monitoring objects and monitoring cycle. When learning load patterns and their related eigenvectors, knowledge base keeps track of operations so that the system's regular operation may be shown.

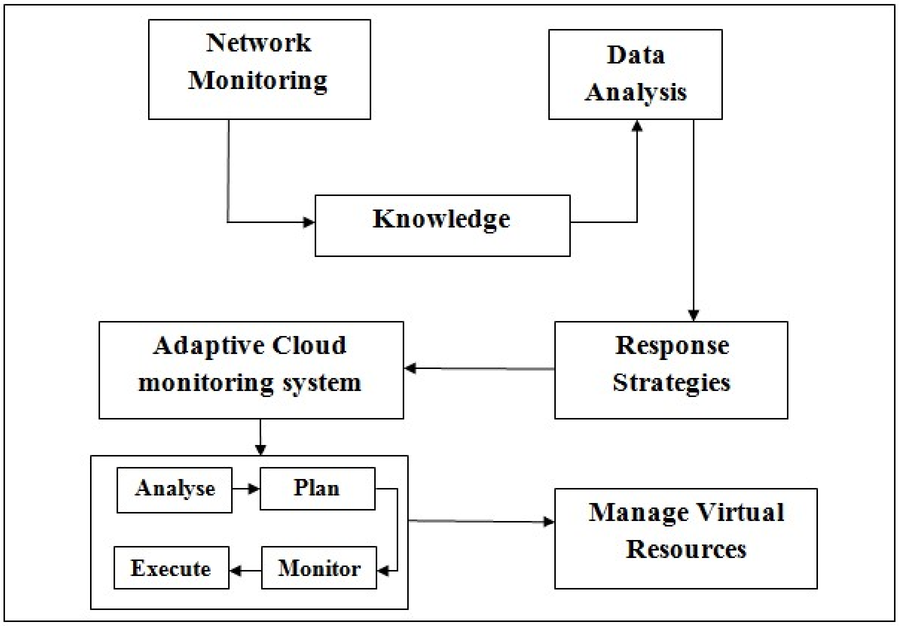

Fig. 1: Framework of Adaptive Cloud Security System

In cloud computing monitoring system different resources are monitored and collaborated with virtual environment. There are two situations mainly describes the virtual environments they are master mode and work mode. In master mode the data is monitored and received with periodic transmission. In work mode the cloud computing monitoring system monitors primary resources which are periodically relay on them. Many elements are generated with the phrase event driven manner where old work nodes will be maintained based on primary resources.

Based on the storage analysis different functions are coordinated with each other in the environment of cloud computing. Next, a model for data acquisition and analysis is established, comprising elements for data gathering, preprocessing, analysis, storage, and other functions. The original data stream is categorized after the data gathering procedure, and the original data are created. To prepare these initial data, the data preprocessing technique is utilized. Finally, the usable data are collected from the enormous data through storage components and the data analysis. The data may be used directly by consumers thanks to these processes and software. This data analysis and gathering strategy creates a seamless data processing system.

Data Collection: Three processes make up the data gathering process in the cloud computing environment: data filtering, data categorization and data capture. Based on the consumer data these three phases will work. After data has been collected, it needs to classify the remaining data and filter out any irrelevant information. The data categorization is then forwarded to the preprocessing section.

Data Preprocessing: Data cleansing, data integration, data transformation, and data reduction are some of the techniques used in data preparation. By providing attribute names and attribute values selection process is made. Based on the original data creation, numerous data source and feasible attributes are performed. This process helps to choose best monitoring system.

Analysis of data: Based on functions of pertinent and suitable circumstances creation of data collecting model is done. Based on the outcomes of anticipation data gathering model is designed. Verification and measurement should be done based on basic model. Based on the validating findings model is changed successfully. Methodology of data collection is also workable. The data which is obtained will be finally cleared out by providing casual link. At last additionally, the data model's construction must be continually refined.

IV. RESULTS & DISCUSSION

The below table (1) shows the comparison of parameters for both cloud computing monitoring system and adaptive cloud security framework. In this cost, network traffic, monitoring period and system security parameters are utilized.

Table. 1: Comparison of Parameters

S.No	Parameter	Cloud Computing Monitoring System	Adaptive Cloud Security Framework
1	Cost	41%	11%
2	Network Traffic	81%	19%
3	Monitoring Period	58%	8%
4	System Security	32%	93%

The below figure (2) shows the comparison of cost and system security for both cloud computing monitoring system and adaptive cloud security framework. In this compared with cloud computing monitoring system cost is reduced and security is increased for adaptive cloud security framework.

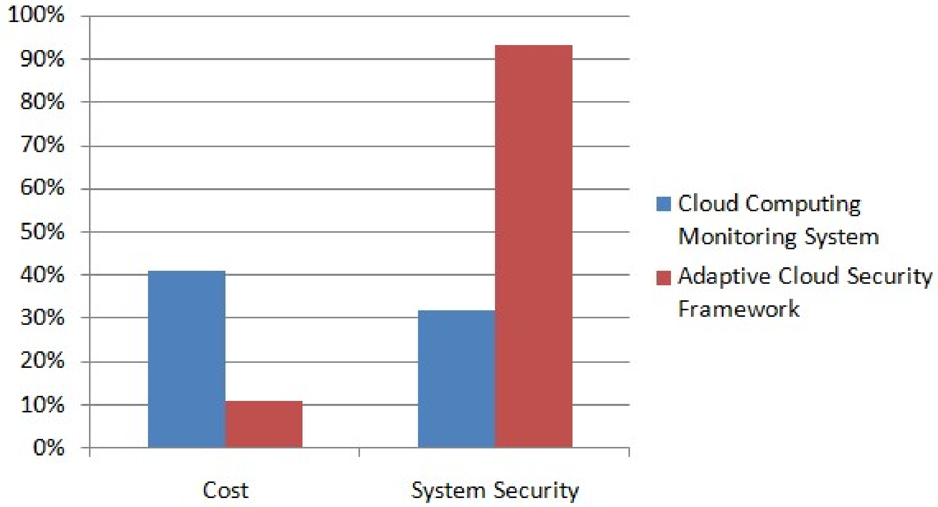

Fig. 2: Comparison of Cost and System Security

The below figure (3) shows the comparison of network traffic and monitoring speed for both cloud computing monitoring system and adaptive cloud security framework. In this compared with cloud computing monitoring system network traffic and monitoring speed is increased for adaptive cloud security framework.

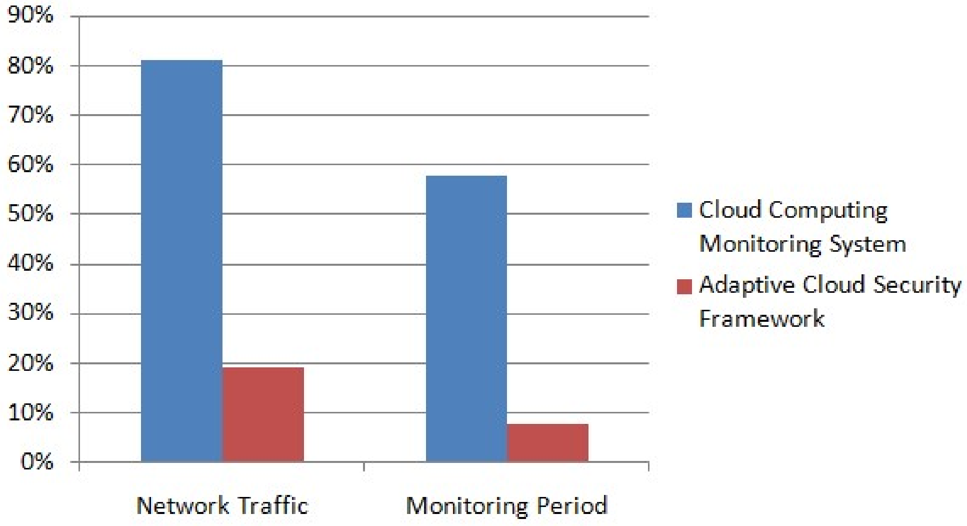

Fig. 3: Comparison of Network Traffic and Monitoring Speed

V.CONCLUSION

The challenge of data security on cloud platforms is never-ending. This draws conclusions from the way autonomous computer systems function and the concept of anomalous data mining. Then, we provide an autonomic computing-based strategy for monitoring data security. To protect the security of cloud platforms, this approach tracks data changes there. The output of the simulation demonstrates that the cost may be decreased based on monitoring cycle adjustment modules by integrating the data collecting, monitoring service, analysis and data volume. The suggested solution, however, does not yet take into consideration the capacity to restore the damaged data. Therefore, future work will take into account the data recovery study and related implementation.

REFERENCES

[1]. R. Choubey, R. Dubey, and J. Bhattacharjee, “A survey on cloud computing security, challenges and threats,” Int. J. Comput. Sci. Eng., vol. 3, no. 3, pp. 1227–1231, 2016.

[2]. R. P. Padhy, M. R. Patra, and S. C. Satapathy, “X-as-aService: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure and Force.com,” Int. J. Comput. Sci. Telecommun., vol. 2, no. 9, pp. 8–16, 2016.

[3]. G.K. Ravikumar “Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing”, International journal of engineering science and Technology, vol. 3, no. 6, pp. 5150-5159, 2015.

[4]. A. Behl, K. Behl, “An Analysis of Cloud Computing security issues,” 2013 World Congr. Inf. Commun. Technol., pp. 109– 114, 2013.

[5]. D Chopra, D Khurana, K Govinda, “CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION,” International Journal of Advances in Engineering Research, vol. 3, no. 2, 2012.

[6]. G. R. Vijay, “An Efficient Security Model in Cloud Computing based on Soft computing Techniques,” vol. 60, no. 14, pp. 18–23, 2012.

[7]. H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, “Threat as a Service?: Virtualization's Impact on Cloud Security,” no. February, pp. 32–37, 2012.

[8]. K. Kumar, V. Rao, S. Rao, and G.S. Rao, “Cloud Computing : An Analysis of Its Challenges & Security Issues,” IJCSN,vol. 1, no. 5, 2012.

[9]. K. D. Kadam, S. K. Gajre, and R. L. Paikrao, “Security Issues in Cloud Computing,” Proceedings published by International Journal of Computer Applications,pp. 22–26, 2012.

[10]. M. Shrawankar, A. Kr. Shrivastava “Comparative Study of Security Mechanisms in Multi- cloud Environment,” vol. 77, no. 6, pp. 9–13, 2011.

[11]. N. Aggarwal, P. Tyagi, B. P. Dubey, and E. S. Pilli, “Cloud Computing : Data Storage Security Analysis and its Challenges,” vol. 70, no. 24, pp. 33–37, 2011.

[12]. P. Aggarwal, M. M. Chaturvedi, “Application of Data Mining Techniques for Information Security in a Cloud: A Survey,” Int. J. Comput. Appl., vol. 80, no. 13, pp. 11–17, 2010.

[13]. A. Botta, W. De Donato, V. Persico, and A. Pescape, “On the integration of cloud computing and internet of things,” Proc. - 2014 Int. Conf. Futur. Internet Things Cloud, FiCloud 2014, pp. 23–30, 2010.

[14]. D. Panth, D. Mehta, R. Shelgaonkar “A Survey on Security Mechanisms of Leading Cloud Service Providers,” Int. J. Comput. Appl. , vol. 98, no. 1, pp. 24–34, 2009.

[15]. D. Porwal, P. Mohmood Khan and D. Shankar Ray, “Cloud Computing Security Threats and Countermeasures”, International journal for innovations in Engineering Science and Management, vol. 2, no. 4, pp. 1-4, 2009.