AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 1(2025)
www.ajmimc.com

ENERGY-EFFICIENT SECURITY MECHANISMS FOR CLOUD COMPUTING: A GREEN COMPUTING APPROACH

K Spurthi[1], B. Premaja[2]

[1]Assistant professor, Swarna Bharathi institute of science and technology, Khammam
[2]Assistance professor. Swarna Bharathi institute of science and technology, Khammam
kolluspoorthy03@gmail.com[1], premaja.b@gmail.com[2]

ABSTRACT:

Cloud computing is increasingly utilized by organizations to store vast amounts of data, including text, audio, and video. As a result, securing this data has become a critical concern. Security remains a significant barrier to the widespread adoption of cloud computing. This paper addresses the security challenges faced by cloud computing systems and proposes a solution through a quantitative security risk assessment model, the Multi-dimensional Mean Failure Cost (M2 FC). Initially, we identify and discuss the key security issues inherent in cloud environments. We then introduce a comprehensive framework for analyzing and evaluating these security challenges. Finally, the paper suggests appropriate countermeasures and strategies to mitigate risks, enhancing the overall security of cloud computing systems.

Keywords: Cloud Computing, Data Security, , M2 FC, Security Framework, Cloud Security

1.0 INTRODUCTION

The term "Cloud Computing," as defined by the National Institute of Standards and Technology (NIST), refers to a comprehensive and rapidly evolving technology that has become integral to daily life. It provides on-demand web services such as networking, storage, servers, and applications, offering flexibility and cost efficiency for users. Cloud computing enables users to scale storage capacity up or down without the need for investment in new infrastructure. The cloud storage process consists of four layers: the storage layer, which houses data in cloud data centers; the management layer, which ensures the privacy and security of cloud storage; the application interface layer, which offers cloud application services; and the cloud access layer, which facilitates user access to the cloud.

Cloud models are typically classified into different service types: Infrastructure as a Service (IaaS), which is the most prevalent cloud service model, providing customized infrastructure on-demand; Platform as a Service (PaaS), which offers a platform and environment for developers to build cloud applications that are stored and accessed via web browsers; and Software as a Service (SaaS), which delivers applications running on cloud infrastructure, where users do not manage or control the underlying cloud infrastructure, including storage, operating systems, services, or networks.

While cloud computing enables the growth of data at an exponential rate, data security remains a significant concern. As data is transferred to cloud data centers, security issues arise, and data owners often lose control over their information. Security and privacy for cloud data are paramount but still unresolved challenges. These include issues such as unauthorized access, data leakage, and the potential exposure of sensitive user information.

1.1 Energy-Efficient Security Mechanisms for Cloud Computing

Energy-efficient security mechanisms for cloud computing aim to reduce both the energy consumption and security risks associated with cloud infrastructure. As cloud computing environments scale to meet growing data demands, securing data without significantly increasing energy usage becomes critical. By integrating energy-efficient algorithms and techniques, such as lightweight encryption methods and energy-aware access control protocols, cloud providers can enhance security while minimizing environmental

impact. These mechanisms not only ensure the protection of sensitive data but also contribute to sustainability efforts by reducing the carbon footprint of data centers, aligning security practices with green computing principles.

1.2 Significant of the work

This work provides a crucial contribution to cloud computing by addressing the persistent security challenges that hinder its broader adoption. By introducing the Multi-dimensional Mean Failure Cost (M2 FC) model, the paper offers a quantitative approach to assess and mitigate security risks in cloud environments. The proposed framework not only enhances the understanding of security issues but also provides practical countermeasures that can be applied to improve data protection. Ultimately, this research paves the way for more secure, energy-efficient, and reliable cloud computing systems, fostering greater confidence and trust among organizations that rely on cloud storage.

2. REVIEW OF LITERATURE

To introduced the concept of cloud computing and its associated services including storage, servers, apps, networks, and services—without actually receiving them. A decrease in risk, data leakage, and other overhead has been seen in the big system, according to the paper's observations [1]. via cloud computing, online services are made available on demand. For businesses that would rather not spend much in infrastructure and deal with issues like hardware and software flaws, machine failure, and disk failure, the cloud is the ideal option. [2] Users may pay as they go for the services they use in the cloud, eliminating the need to invest in costly infrastructure, claims this report. Data is expanding at an exponential rate, but the safety of these open-ended and relatively easily accessible resources is still up for debate. This article delves into the security risks associated with the cloud, its features, its delivery model, and its stakeholders in 2012. Cloud security was the topic of the writers' brief. Concerns about the security of cloud networks have grown in recent years due to the increasing number of users entrusting these services with sensitive information and the volume of network traffic they generate, receive, and keep. [5] Throughout the preceding piece of writing, the author delves into a certain Threats to cloud security include data corruption, man-in-the-middle attacks, and the disclosure of sensitive information. Due to its adaptability, cost-effectiveness, and the ability to change data between clients and servers, cloud computing has emerged as one of the most active areas of technical development. In order to keep the information-containing transaction table up-to-date and to guarantee robust data security, this article elaborates on how to use a reputation management system. Cloud computing relies on virtualization; however virtualization security has not been well investigated [7]. This article examines cloud security from a virtualization attack perspective, specifically looking at how various cloud computing service models are impacted. Through the use of virtualization, cloud computing offers a platform for the sharing of resources, including software and infrastructure [8]. The goal of discussing cloud computing is to create an environment that can reliably and flexibly deliver services. Which, when discussing cloud environments, strive to be both dependable and adaptable in their service provisioning. Data stored in the cloud is encrypted using the RSA method and digital signatures as part of the cloud security protocol, with which all cloud service providers must comply. This study primarily focuses on the usage of multi-clouds, reducing security threats, and improving data security during network data transfers [9]. It also describes security management frameworks, standards, and the RSA algorithm with digital signature to enhance cloud data security [10]. When users transfer data outside of organizational boundaries and access them over the internet, it results in a loss of control for the owner.

3.0 RESEARCH METHODOLOGY

This study employs a quantitative research methodology to assess and address security risks in cloud computing systems. The approach begins by identifying and categorizing the key security vulnerabilities prevalent in cloud environments. We then introduce the Multi-dimensional Mean Failure Cost (M2 FC) model as a tool for quantifying the costs associated with these risks. To evaluate cloud security, we develop a modular framework that enables systematic analysis of each identified threat. This framework allows for the implementation of targeted security measures to mitigate risks, which can then be compared in terms of effectiveness using the M2 FC model. The research involves both theoretical development and practical implementation, where the proposed system is tested in real-world cloud computing environments. Data collected during the implementation phase will be used to validate the proposed methodology, assessing the impact of different security countermeasures on overall cloud system security and cost reduction

M2 FC MODEL: In introduced a quantitative security risk assessment measure that quantifies this risk in terms of financial loss per unit of operation time (for example dollars per hour ($/h)) due to security threats considering several dimensions within the threat world. The measure is called as the Multidimensional Mean Failure Cost (M2 FC). The M2 FC is a stakeholder-based security threats assessment model. It estimates the security of a system in terms of the loss that each stakeholder incurs due to security breaches considering several dimensions within the threat world. In fact, the world of security threats is a segmentation of this world according to each of its dimensions where a dimension can be defined as an elementary aspect or extent of the threat word. The domain or world of threats can be perceived as having several dimensions like architectural components, environmental elements, time, deployment site…For example, when considering the deployment dimension; we give the mean failure cost per deployment site where a security breach occurs. The basic idea is to consider threat perspectives to estimate security failure. To better explain the usage of the proposed M2 FC model, we apply on a case study to estimate the security of a system in terms of loss incurred by each stakeholder

Proposed Framework: After introducing security issues in cloud computing system, we need to make approach that allows analyzing and making relation between security problems and their solutions. We notice that some investigators proposed solutions to threats but, they didn't relate solutions to security issues. We propose, in this section, an approach that uses quantitative analysis in order to ensure that our results are more logical and efficient.

Security Issues in Cloud Computing:

There are numerous parts in cloud computing like applications, platforms and infrastructure. Every one of them contains a completely different functionality and might supply differing types of services and products. A lot of variety of applications of cloud suggests that there would be a lot of security problems. The integration of various parts and technologies makes it difficult to own a secure cloud service. A number of these services are databases, virtualization, operating systems, networks, scheduling, transactions, backups, load balancing, concurrency and memory management. There is also completely different security problems for every of the systems and technologies. For example- The information must be secure because it contains all the sensitive information stored by the user and it may be attacked or infiltrated by a hacker. All information shouldn't solely be encrypted however it ought to be madesure that there are specific protocols and policies once information is shared and retrieved or stored

Security Issues in Virtualization: Cloud computing is prone to several concerns related to the use of virtualization technology In fact, CC systems are based on several technologies

like distributed systems, utility computing and virtualization. This last technology allows several security harms in this system and lets many new security threats like VM-based rootkits attack which is designed to infect both client and server machines in the cloud. It abuses compromised systems by hiding files and registry keys and other operating system objects from diagnostic.

Methods For Securing Rough Data Set:

Genetic Algorithm: Genetic Algorithm (GA) is a searching technique that is used to find approximate or exact solution to optimization and search problem GA convert distinct domain problem to a model by using chromosome and the algorithm process starts with a random selection of the population of chromosomes. Chromosomes are converted into bits or numbers according to the problem

K-Mean Algorithm: K-mean is the easiest algorithm of partitioning method for clustering analysis. The aim of this algorithm is to minimize an objective function known as square error function is given below

$$J = \sum_{i=1}^{K} \sum_{j=1}^{Ki} (\| Pi - Ci \|)^2 \quad (1)$$

‖Pi − Ci‖ is Euclidean Distance between Pi and Ci

„k" is the number of cluster centers

„ki" is the number of data points in i^{th} cluster.

Algorithm for k-Mean Algorithm Let P={p1, p2, p3, p4, p5, ……., pn} is the set of data points and C={c1, c2, c3, c4, c5, …, cn} is the set of center.

- Randomly select K points as initial value of the cluster center
- Calculate the distance between each data points and cluster centers
- Assign each data points to the cluster of the nearest points measured with a specific distance metric.
- Re-compute new cluster center using

$$Ci = (1/Ki) \sum_{j=1}^{Ki} Pi \quad (2)$$

KNN (K- Nearest Neighbor) Algorithm KNN Algorithm is used for both classification and regression predictive problems and based on feature

similarity: choosing the correct value of k is a process called parameter tuning that is important for better accuracy. Pseudo code for KNN Algorithm

- Initialize k from your chosen number of neighbors
- Calculate distance between the points using Euclidean distance
- Arrange the calculated Euclidean distance in ascending order.
- Select the first k entries from the sorted list.
- Find those k-points corresponding to these k-distances.

4. SECURITY TECHNIQUES FOR SECURING CLOUD:

Cloud security measures include firewalls, intrusion detection systems, obfuscation, tokenization, VPNs, and staying away from public Wi-Fi. One subset of cybersecurity is cloud security. When it comes to data that may rely on cloud security, cloud encryption isn't the way to go. Making it is as simple as using preexisting security measures like Cloud data may be protected using any number of methods, including authentication and identification, encryption, integrity checking, access control, secure detection, and data masking.

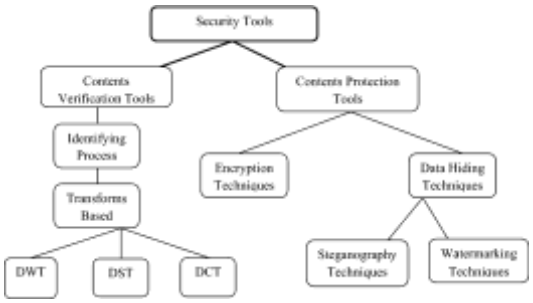

Figure 1: Explains security techniques.

We applied in this section our framework to an illustrative example named cloud computing system. We applied the M2 FC model to quantify cloud systems and estimate the financial cost for each stakeholder regarding the architectural component and deployment site dimensions. In fact, we take into account the deployment sites dimension and the

architectural components dimension. Our assessment varies.

Security Threats: Components of the architecture may fail to operate properly as a result of security breaches due to malicious activities. Therefore, we specify, in this step, the catalog of threats that causes components failure. We select for each component, the higher probabilities that in which a component Ck fails once threat Tq has materialized. We will present threats that affected components above, through an analysis of probabilities of failure components matrix

Table 1. Probabilities of failure requirements for sites

Security requirements	Probabilities of failure requirements for sites Step-1			
	browser	**Web_ server**	**Proxy_ failure**	**No failure**
Availability	0,2	0,1	0,3	0,4
Confidently	0,1	0,1	0,2	0,6
integrity	0,1	0,2	0,4	0,3
Probabilities of failure requirements for sites Step-2				
	browser	**Web_ server**	**Proxy_ failure**	**No failure**
Availability	0,2	0,3	0,3	0,5
Confidently	0,3	0,3	0,3	0,7
integrity	0,2	0,2	0,2	0,6

- In integrity case, we find that the higher probabilities of impact of attack with the following components: Browser, proxy server and web server;
- In availability case, we find that the higher probabilities of impact of attack with the following components: Browser, proxy server and web server;
- In confidentiality cases, we find that the higher probabilities of impact of attack with the following components: Browser, proxy server and web server.

Thus, we will consider in this illustration two dimensions in cloud computing systems namely deployment sites and architectural components. As well, we consider as a leading dimension the deployment site dimension. Thus, to illustrate our secure framework, we will consider mainly these two dimensions. Therefore, we consider that the considered system is deployed on two sites. We have S = {S ite1, S ite2} and the component dimension D has the following elements which is equals to D = {Browser, Web server, Proxy server}. We identify as well two stakeholders for this example namely: local user and external user. We consider that this system is prone to four kind of security threats hence the set T = {Virus, Data Bases Attacks, Denial of service}. Finally, as we mention in the illustrative example in (Jouini & Ben Arfa Rabai, 2015) that we consider the following requirements R = {Availability, Integrity, Confidentiality}. Since the failure of security requirement depends on which component of the system architecture is operational, we will identify in this step using probabilities of failure requirements matrix (PFRs) for each security requirement components causing this failure

CONCLUSION:

The primary goal of this article is to help users identify potential security risks associated with their cloud computing systems by categorizing and emphasizing the most critical issues in this domain. We propose a quantitative methodology for analyzing and evaluating cloud computing security vulnerabilities. Our suggested framework is designed to be modular, allowing for the gradual addressing of security threats. This modular approach enables administrators to implement targeted solutions to mitigate risks and enhance cloud system management. To develop a comprehensive security assessment and management system that can be seamlessly

integrated into cloud computing services to meet security requirements. Following the development of this system, we plan to implement it in real-world cloud computing environments. Additionally, we will manage the M2 FC model by comparing the costs of various security countermeasures with the benefits they bring, demonstrated by the reduction in M2 FC values.

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, 2011.
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, 2011.
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, 2011.
4. A. Behl, K. Behl, "An Analysis of Cloud Computing security issues," 2012 World Congr. Inf. Commun. Technol., pp. 109– 114, 2012.
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, 2013