International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 4th Aug 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-08

DOI: 10.48047/IJIEMR/V10/I08/01

Title **DESIGN AND DEVELOPMENT OF HOME AUTOMATION SYSTEM FOR CONTROLLING ELECTRICAL APPLIANCES**

Volume 10, Issue 08, Pages: 1-7

Paper Authors

Mr S. CHOUDAIAH, Mr BAKA KAMALESH

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN ANALYTICAL APPROACH AND CLOUD SECURITY IN CLOUD COMPUTING

Mr S. CHOUDAIAH, Assistant Professor, **Dept of MCA,** SVIM - Sree Vidyanikethan Institute of Management, Tirupati.

Mr BAKA KAMALESH, VIth semester, Dept of MCA, SVIM - Sree Vidyanikethan Institute of Management, Tirupati.
Email.id: kamalesh1998.kb@gmail.com

ABSTRACT

In today's research environment, cloud computing is becoming more popular. The flexibility, domain compatibility, and improved service utilisation are the key advantages of cloud computing. As a result, the application of cloud computing in various domains is its primary strength, along with the simplicity with which resources may be shared. The growing use of cloud computing has resulted in a wider range of user-data security concerns. In this work, an empirical meta-analysis in the area of cloud computing security is presented. It also provides a comprehensive discussion based on the study's findings. This study examines cloud computing security from both an analytical and empirical standpoint. Data security, data management, and an effective resource sharing method are among the key topics discussed in this article. It also includes the computational aspects of the research and analysis, as well as their applicability. It considers a broader perspective and the range of applications in many domains, as well as the simplicity of data administration and safe data exchange mechanisms.

***Keywords*— Cloud computing, Computational approach, Analytical approach, Data security, Data management**

I INTRODUCTION

Cloud computing is the next generation of internet-based, highly scalable distributed computing systems that deliver computational resources "as a service." “A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction,” according to NIST. The cloud model has two essential characteristics: multitenancy and elasticity. Multi-tenancy allows several tenants to share the same service instance. Elasticity allows a service's resources to be scaled up and down in response to current service needs. Both features are aimed at maximising resource usage, lowering costs, and increasing service availability. Industry and academics have embraced cloud computing to host a broad range of applications, from computationally heavy applications to lightweight services, thanks to the cloud model. Small and medium enterprises will benefit from the approach since it allows them to embrace IT without having to spend in infrastructure, software licencing, or other necessary items up front. Furthermore, governments are becoming increasingly interested in the potential for cloud computing to decrease IT expenses while also increasing the capabilities and reachability of their offered services.

According to a Gartner report on cloud computing sales, the cloud market was valued USD 58.6 billion in 2009, USD 68 billion in 2010, and USD 148 billion by 2014. Cloud computing appears to be a viable platform based on these figures. On the other side, it piques attackers' interest in exploiting any existing flaws in the model. Despite the potential benefits and profits that the cloud computing model might provide, there are still a number of unresolved concerns that affect the model's creditability and pervasiveness. The cloud computing paradigm has a number of open research challenges, including vendor lock-in, multi-tenancy and isolation, data management, service portability, elasticity engines, SLA management, and cloud security. Security is a key worry for cloud users that is preventing them from adopting the cloud computing paradigm because:

- Enterprises outsource security management to a third party that hosts their IT assets (loss of control).

- The presence of assets belonging to various tenants in the same area and utilising the same instance of the service while being ignorant of the security restrictions in place.

- The SLAs between cloud users and cloud providers do not include any security guarantees.

- Storing this collection of valuable assets on publicly accessible infrastructure raises the risk of an assault.

II RELATED WORK

In 2017, Navamani et al. examined the current state of cloud computing. They've also talked about the security issues. They claim that attackers can gain access to the vulnerable hosts. They claim that having open ports opens the door to a slew of dangers. The open ports in the cloud computing environment were investigated. For this problem study, they employed Amazon Web Services (AWS). Several concerns and elements have been explored as a result of this. Lufei and Zuoning explored cloud computing in terms of application and infrastructure stacks in 2017. They have examined and investigated the key disadvantages of operating systems. It is built on a cloud computing platform. There has been a proposal for an operating system architecture. It's for use in a cloud-based computer environment. vStarCloud is the name of their proposed environment.

It is useful for managing virtual machines. Jujare explored cloud computing in relation to grid computing and distributed computing in 2018. This provides extensive IT administrations to clients on a pay-per-use basis, according on the client's requirements. In actuality, it is the administration provided by a third-party vendor that claims the framework. Clients may use distributed computing to develop a variety of apps, store data in the cloud, and access it from anywhere on the world. The issue is, the data must remain secure in its current location, thus security is a major concern in distributed computing.

Gordin et al.discussed public cloud services in 2018. According to the authors, security is the primary worry in the cloud computing environment when it comes to communication. They conducted a security assessment of the OpenStack Pike release. It may be done both inside and outside. They also examined the isolation of hypervisor-based virtual machines. The multi-tenant situation has led to this conclusion. Sharma et al. investigate cloud computing in terms of data transmission and sharing storage and repository in 2019. They have offered a storage facility for cyberspace data that may be used as a service to its users. They have argued that data security is required because the data is kept on many mediums. They have proposed that data security and privacy protection are necessary.

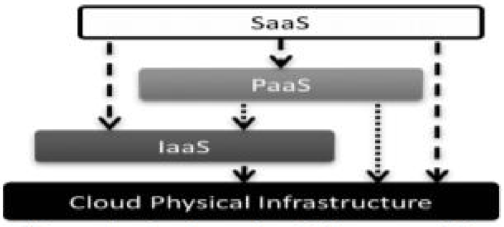
III IMPLEMENTATION

There are three service delivery methods and three major deployment models in the Cloud Computing paradigm. The three deployment models are: (1) private cloud: a cloud platform dedicated to a single organisation, (2) public cloud: a cloud platform open to the public for registration and use of available infrastructure, and (3) hybrid cloud: a private cloud that can extend to use resources in public clouds. Because public clouds are open for public users to host their services, including malevolent users, they are the most susceptible deployment model. The following are examples of cloud service delivery models, as shown in Figure 1:

Infrastructure-as-a-service (IaaS): Cloud providers provide compute resources, storage, and networking as internet-based services. The virtualization technology underpins this service architecture. The most well-known IaaS supplier is Amazon EC2.

Platform-as-a-service (PaaS): where cloud providers give platforms, tools, and other business services that let clients to create, deploy, and maintain their own apps without having to install any of these platforms or support tools on their own computers The PaaS paradigm can be built on top of an IaaS model or directly on top of cloud infrastructures. The most well-known PaaS are Google Apps and Microsoft Windows Azure.

Software-as-a-service (SaaS): where cloud providers provide programmes housed on cloud infrastructure as an internet-based service to end users, rather to needing the consumers to install the apps on their PCs. This approach may be hosted on top of PaaS, IaaS, or cloud infrastructure directly. A good example of a SaaS supplier is Salesforce CRM.



As shown in Figure, each service delivery model includes a variety of alternative implementations, complicating the creation of a common security model for each service delivery model. Furthermore, various service delivery models may coexist in a single cloud platform, complicating the security management process even further.

Cloud implementation

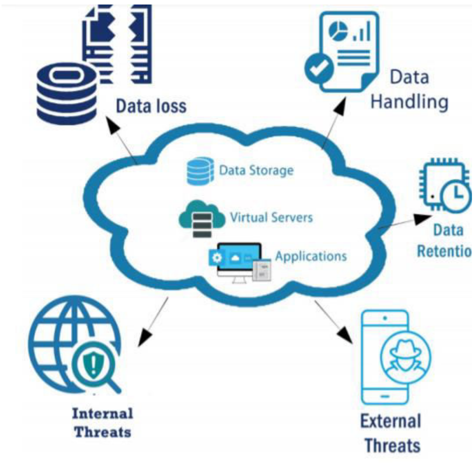
To begin, we'll import the TensorFlow library into Google Colab and make a Tensorflow library object. Then we use Keras to obtain a training dataset and import the matplot and other necessary libraries. Following the import of Keras, we label the objects in the data set, followed by the pre-processing of training pictures. The data is then analysed and an inference is generated using convolutional flatten and max pooling layers. The accuracy, loss, and time per sample of the models are then obtained in order to construct a model.

Create a categorization model and get the results you need. The concept is implemented here using 10 – 1000 Epochs. The number of training instances each training attempt for a model with the same training data set is specified as epoch in this approach. The notion of Epoch is used to show the Caching optimization approach, which refers to the caching of frequently used pictures on a user's local drive. We presented four alternative security encryption methods for data security to analyse the security factors.

IV METHEDOLOGY

Process flow

The method was adopted in the same way that the pilot study was performed to guarantee that the project ran well. Prior to beginning the project, a study was conducted to determine project specifications, cost estimates, resources needed, and a schedule. The project requirements include a thorough examination of the various protocols in two distinct topologies in terms of throughput, average delay, accuracy, loss function, complexity, and security. We are particularly pleased to see that our project is quite cost-effective, as we are utilising readily available resources in our department laboratories. For the cloud simulations, we're utilising the Tensorflow library in Google Colab, which is a free open source platform for cloud computing. We're also utilising Jupyter notebooks on Google Colab for the security parameters. As a result, our anticipated cost is quite minimal, and it just includes the paperwork and other necessary hardware.



Cloud computing

Comparative Study

The end outcome will be a parameter comparison study. The measurement of data and the recording of data into compact tabular representations are both important aspects of our research.

The acquired results are then projected into graphical representations for comparative study. We're using Google Sheets as our primary data analysis tool to complete all of these activities. The programme was used to create a visual representation of the data.

portray the collected results for a better comprehension and inference to draw a conclusion from the findings Separately, we looked at network performance and security factors. On a LAN server-client system that was available, the network characteristics were examined. By developing several algorithms on cloud compilers and measuring the execution times with their complexit, the security parameters were examined. We utilised Google colab as a cloud platform to construct a real-time deep learning classification model with Tensorflow library and retrieve the loss function, accuracy, and training time per sample as a common platform to connect them both.

V CONCLUSION

First, a broad overview of cloud computing and its benefits has been conducted in this work. In the second segment, a security-based meta-analysis was given in order to examine current security trends. Problem statements have been examined based on the patterns. Finally, the findings of the most recent approaches were reviewed and investigated. Based on the study and analysis, a secure framework with an internal auditing system that is integrated with a preventative mechanism to manage internal and external risks is recommended. It is also advised that it should cover data loss management and data retention mechanisms in order to prevent data breaches and losses.

FUTURE WORK

We're looking at the cloud security management issue. Our goal is to close the security gap that has emerged in cloud users' and cloud providers' security management procedures as a result of the cloud model's adoption. To solve this problem, we must: (1) capture different stakeholders' security requirements from various perspectives and levels of detail; (2) map security requirements to cloud architecture, security patterns, and security enforcement mechanisms; and (3) provide feedback to cloud providers and consumers on current security status. In order to address the challenge of cloud security management, we suggest using an adaptive model-based method. Models will aid in the abstraction of problems and the capture of different stakeholders' security needs at various degrees of detail. Adaptability will aid in the delivery of a cloud security paradigm that is integrated, dynamic, and enforced. The feedback loop will track security status in order to improve the present cloud security paradigm and keep cloud users informed about the protection of their assets (applying the trust but verify concept).

VI REFERENCES

1. R. Gargista Gustamas and Guruh Fajar Shidik – Analysis of Network Performance on Cloud Computing , IEEE 2017

2. Cheikh Brahim Ould Mohamed El Mocta and Karim KonatÃ© Survey of Security Challenges in Cloud Computing, IEEE 2016

3. S. Eman Mahmoodi R. N. Uma and KP Subbalakshmi Optimal Joint Scheduling and Offloading for Cloud Computing IEEE 2019

4. G. Sousa, W. Rudametkin, and L. Duchien, Automated setup of multi cloud environments for microservices applications, in Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD), Jun./Jul. 2016, pp. 327334

5. Z. Hao, E. Novak, S. Yi, and Q. Li, Challenges and software architecture for fog computing, IEEE Internet Comput., vol. 21, no. 2, pp. 4453, Mar./Apr. 2017

6. W. Cai, V. C. Leung, and L. Hu, A cloudlet-assisted multiplayer cloud gaming system, Mobile Netw. Appl., vol. 19, no. 2, pp. 144 152, 2014.

7. H. Hong, D. Chen, C. Huang, K. Chen, and C. Hsu, Placing virtual machines to optimize cloud gaming experience, IEEE Trans. Cloud Comput., vol. 3, no. 1, pp. 4253, Jan.-Mar. 2014.

8. T. Verbelen, P. Simoens, F. De Turck, and B. Dhoedt, Leveraging cloudlets for immersive collaborative applications, IEEE Pervasive Comput., vol. 12, no. 4, pp. 3038, Oct.-Dec. 2013.

9. I. 802, Ieee standard for local and metropolitan area networks: Overview and architecture, IEEE Std 8022014, p. 8, 2014.

10. S. Das, M. Khatua, S. Misra, and M. Obaidat, Quality-assured secured load sharing in mobile cloud networking environment, IEEE Trans. Cloud Comput., 2015, DOI: 10.1109/TCC.2015.2457416.

11. M. Aazam and E.-N. Huh, Dynamic resource provisioning through fog micro datacenter, in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops, Mar. 2015, pp. 105110.

AUTHOR PROFILE:

Mr. B. Kamalesh, VIth semester, dept of MCA, Sree Vidyanikethan Institute of Management from SV University., (A.P), INDIA.
Email id: - kamalesh1998.kb@gmail.com