IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105147

DEALING WITH SECURITY ISSUES USING DEPLOYMENT MODELS IN CLOUD ENVIRONMENT

K V Sarath Kumar[1], Nagaraj G Cholli[2]

Student, Information Science, R.V College of Engineering, Bangalore, India[1]

Professor, Information Science, R.V College of Engineering, Bangalore, India[2]

Abstract: Cloud computing is becoming popular in the field of IT industry these days. It's a model that allows people all over the world to connect to shared pools of programmable resources over the internet. That is, it can execute many apps or programs on many computers at the same time. Cloud computing's nature and applications are continually evolving, both virtually and in reality.The deployment of cloud models is explored in this study.The main cloud deployment types are public,private,community and hybrid clouds. Each of these models has its own set of benefits and drawbacks.Cloud computing is successful in providing a cost effective strategy for most of the companies to manage IT. The major thing that is limiting the cloud's expansion is security.In this paper different deployment approaches are proposed depending on various security concerns.. Each model adds to the security measures offered by the preceding ones. The last model alleviates security problems.It can be used as a template for future models.

Keywords: Cloud Security, Cloud Deployment,Separation of Duties,Data migration,Data Confidentiality,Data Integrity,Data Privacy

I. INTRODUCTION

The growing popularity of cloud computing has resulted in a variety of cloud deployment models. Although these models use comparable technologies but differ in terms of reliability,cost and security.The architecture on which a cloud system is implemented is known as a cloud deployment model.Management, ownership, access control, and security standards are all different amongst these types.This means that deployment types differ based on who is in charge of the infrastructure and where it is situated.

The cloud model which is optimal for a company isn't always apparent.While selection one must consider the company requirements, as well as what different deployment models can provide.

II. DEPLOYMENT MODELS

A. Public Cloud

The most extensively utilized cloud service is the public cloud model.The general public has access to public clouds, and data is produced and stored on third-party servers.

In this model service providers are in charge of maintaining and administering server infrastructure so that there is no need for companies to maintain hardware on their own.Provider firms provide resources as a service through the Internet, either for free or on a pay-per-use basis. Users can adjust resource scaling as needed.Businesses with low privacy concerns prefer this deployment model.Examples are Microsoft Azure, Amazon Elastic cloud (EC2), Salesforce heroku , Google app engine etc.

i) Advantages:

1. Hassle free infrastructure management: It's handy to have a third party manage our cloud infrastructure: We don't have to worry about developing and maintaining the software because the service provider does it for us. Furthermore, the infrastructure setup and usage are simple.
2. Reduced costs: As the payment is done only for the services that are used the costs are reduced.
3. No Hardware investment: As service providers will take care of the entire infrastructure there is no need for investing in the hardware resources.
4. High Scalability : It can be scaled according to the requirements of the company.

This work is licensed under a Creative Commons Attribution 4.0 International License

ii) *Disadvantages:*

1. Security and private concerns:This architecture does not provide enough protection against attacks because anyone can request access. Vulnerabilities arise as a result of the public cloud's scale.
2. Reliability:Outages and failures are common in public clouds.
3. Poor customization:There won't be much possibility for customizing this type of cloud. Organizations have to choose their OS and VM size (storage and processors), but ordering, reporting, and networking cannot be customized.

B. Private Cloud

From a technological standpoint, there is very little difference between a public and a private model, as their structures are relatively similar. A private cloud, on the other hand, is owned by only one firm, as opposed to a public cloud that is accessible to the whole public. It's also known as an internal or corporate model for this reason.These infrastructures, regardless of their physical location, are maintained on a dedicated private network and employ software and hardware that is solely meant for use by the owning firm.

In comparison to the public cloud, the private cloud offers more flexibility in customizing the infrastructure to meet the needs of the business. A private approach is particularly well suited to enterprises that need to protect mission-critical activities or have continuously changing requirements.Amazon, IBM, Cisco, Dell, and Red Hat are some of the public cloud service companies that provide private cloud solutions.

i) *Advantages:*

1. Customization: Customization can be done as per the requirements of the company.
2. Data privacy: Data can only be accessed by approved internal people. It's ideal for keeping company information.
3. Full control:The owner will be responsible for the integration of services, operations, policies etc. The company is the only owner.
4. Support for Legacy systems: Legacy systems can be built on private cloud.Public cloud model doesn't support Legacy systems.

ii) *Disadvantages:*

1. Extensive cost : Money has to be spent on hardware and software, as well as budget for in-house staffing and training.
2. High maintenance: High maintenance is required as a private cloud is managed-in-house.

C. Community Cloud

This model is mostly similar to the private one except that there is a difference in the set of users.The infrastructure and associated resources of a community cloud are shared by numerous organizations with comparable backgrounds, whereas the infrastructure and associated resources of a private cloud server are owned by just one corporation.
When all of the participating firms share the same security, privacy, and performance needs, as in cooperative projects, this multi-tenant data center design can help them improve their efficiency. The creation, administration, and implementation of projects are all made easier with a centralized cloud. All users are responsible for the fees.

i) *Advantages:*

1. Reduction in cost:When compared to corporate cloud this cloud is quite cheaper while providing equivalent performance. The cost of these solutions is further reduced by the fact that many firms split the expense.
2. There is improvement in data privacy and security aspects.
3. Exchange of data can be done easily.

ii) *Disadvantages:*

1. Shared resources: Within community systems, limited storage and bandwidth capacity are typical issues.
2. Uncommon : This model is not often used yet.

D. Hybrid Cloud

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI 10.17148/IJARCCE.2021.105147

As with any hybrid phenomenon, the best aspects of the previously described implementation types are included in the hybrid Cloud (public, private and community). It allows firms to combine and match the three sorts of features that best fit their needs.

By placing the task's crucial workload on a secure private cloud and implementing those that are not so sensitive to the public, an organization may balance its load. In addition to guaranteeing and controlling strategically essential assets, the hybrid cloud deployment approach makes them cost-effective and resource-efficient. This method also promotes mobility of data and applications.

Cloud bursting frequently uses the hybrid cloud approach. Cloud bursting allows a company to operate apps on-premises but "burst" onto the public cloud when the workload becomes too much. It's a great choice for companies with a variety of use cases.

i) *Advantages:*

1. Cost - effectiveness: This solution lowers the operational costs as it uses a public cloud for most of its needs.
2. Flexibility: This cloud-based solution provides a lot of configuration flexibility. Clients can design unique solutions that are completely tailored to their requirements.

ii) *Disadvantages:*

1. Complexity : As it involves two or more infrastructures it is quite difficult to set up the system and manage.
2. Specific use case: This methodology is only efficient if organizations can divide their data into mission-critical and non-critical ones.

III. Cloud Security Issues

Many companies do not adopt cloud computing stating various reasons which include virtualization,Loss of IT infrastructure control etc.The user's security issues are given as:

A. *Separation of Duties*

It is an increasingly common concept that requires more than one person or component to complete the work or task so that there is a reduction in fraud occurrence.As a consequence, division of roles collapses collaboration between entities to compromise the system.

B. *Availability of Data and Service*s

Availability will make sure that the relevant persons have reliable, steady, and timely access to data or resources. It guarantees that the systems are operating properly and that connectivity is available whenever it is required, as well as allowing authorized people access to the systems or network .Uptime is another term for availability and it refers to availability of service.

C. *Data migration*

Data migration is a process in which the data is moved from one place to another or from one application to another or from one format to another. Migration is the process of moving services and applications from one cloud vendor to another.To transfer information(data) automatically different programs are used.

D. *Data Integrity*

Data integrity is an assurance that data will be preserved in the same way during any action, such as storage,retrieval and transfer. Data integrity makes sure the data is accurate and trustworthy.There is no universally accepted standard to maintain integrity of data.It refers to the preservation of completeness and meaning of the data.

E. *Data Confidentiality*

The process of securing data against unauthorized access and disclosure by the outsourced server and unauthorized users

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI 10.17148/IJARCCE.2021.105147

is known as data confidentiality. This is accomplished by encrypting the data and allowing only authorized users to decrypt it.Because of the public nature of the cloud, it is important. In order to offer secrecy to users' data, some restrictions must be provided at various cloud tiers . Confidentiality protects information against unlawful disclosure, whether intentionally and unintentionally.

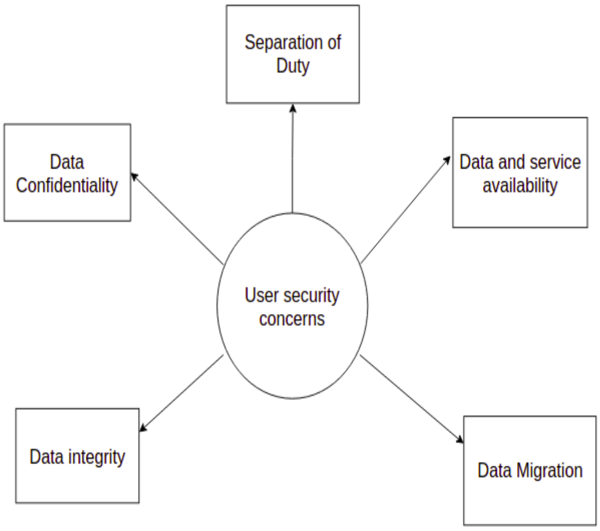

Figure 1: User security concerns

IV. Proposed Models

Three different types of modules of participants can be used to describe cloud computing scenarios: users, services, and the cloud provider.Each participant role is to provide a specific type of interface to other participants.Let us consider a base model and improve this model so that our requirements are fulfilled.Along the way the advantages and disadvantages For each model disadvantages are expressed.

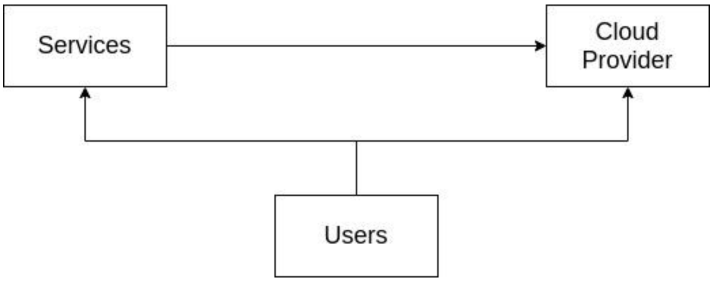

Figure 2: Base Model

Separation Model

In Separation model first security issue i.e separation of duty concept is covered.In this first data is processed after that it is stored.Here, both the processing section and storage section are sectioned apart.The processing of data is handled by one section whereas the storing of data is handled by the other.

In this model the service provider is incharge of either storage section or the processing section but not both simultaneously.This is done to make sure that the provider doesn’t have more control This is done to prevent provider from having extra control over the data due to which the security is improved.

Drawbacks:

1. Service providers can still identify one another, collusion is feasible, and communication filtering between various service providers is impossible.

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI 10.17148/IJARCCE.2021.105147

2. If the user wants to change the service provider and the new service provider is not compatible with the present data then the data might be lost or it might be in non working state.

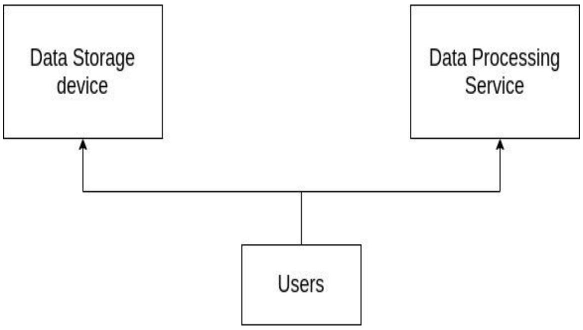

Figure 3: Separation Model

A. Availability Model

In cloud computing service availability is one of the major concern for the users.In this model at least two data storage devices and two distinct data processing services are used.Data processing and storage are no longer under any service provider simultaneously.Synchronization and replication of data is done by the Duplication service.There won't be any failure in accessing of data as backup is present in this model.

Drawbacks:

1. Storage and Processing sections are redundant in nature which leads to increase in the cost when compared to the segregation model.
2. Data migration problem still exists here.
3. There is no evidence that this model covers integrity and confidentiality aspects of the data.

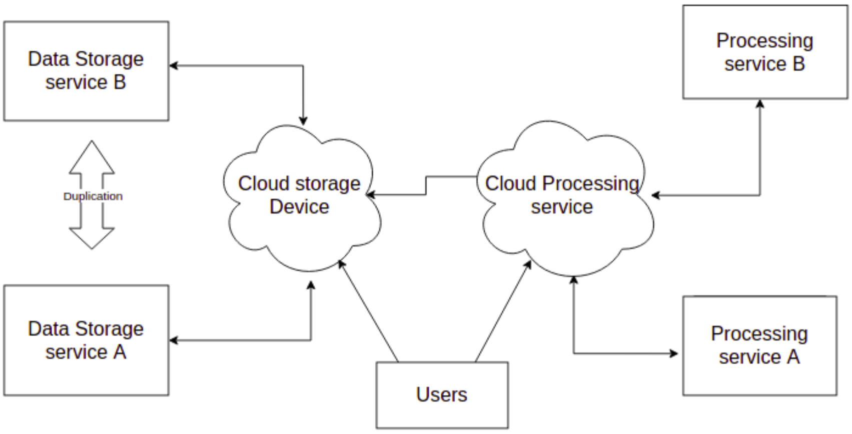

Figure 4: Availability Model

B. Migration Model

Data migration is a process in which data might change its format or it gets moved from one device to another.It becomes essential when a user wishes to make use of a new DBMS or computing systems which is not compatible with the present system.Transferring of data is carried out by a set of scripts or programs that perform the action of transferring the data automatically.

The interaction is achieved between storage services in the cloud migration service model. Users no longer have to be concerned about a cloud service provider having complete control over their data.
Drawbacks:
1. It only covers SOD,availability,data migration and fault tolerance.

This work is licensed under a Creative Commons Attribution 4.0 International License

2. There is no assurance that the data protection in this model is adequate to safeguard data integrity, and confidentiality is not included.

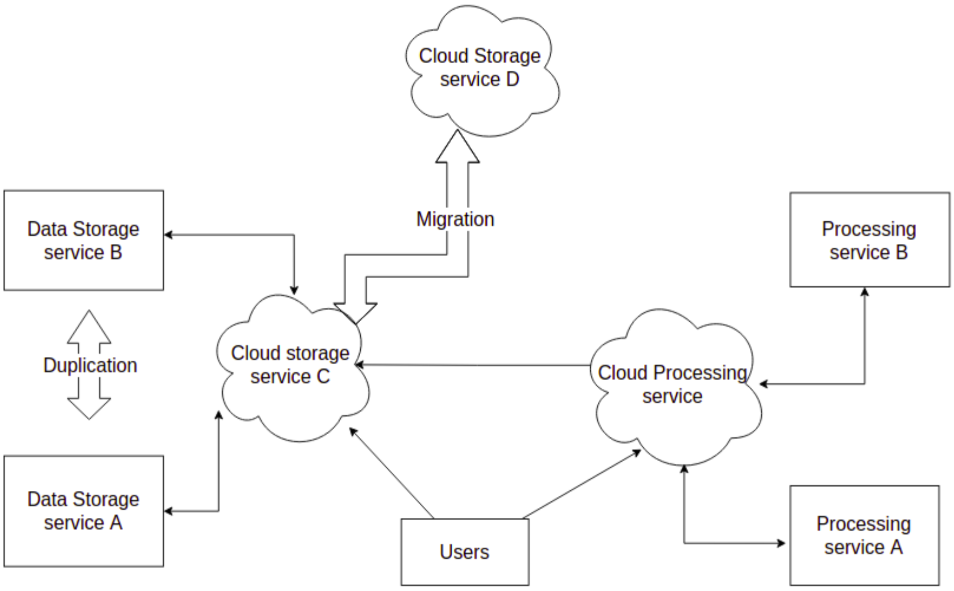

Figure 5: Migration Model

C. Tunnel Model

In the previous model as service providers communicate directly with one another, data security is compromised and the system is unreliable.User data gets altered in the data processing section and moved to the storage section to get stored.The alteration of data depend on the interface provided by the tunneling section.Based on the interface, the data that is saved differs from the data in the data processing service. As a result, data stored by a cloud storage service cannot be linked to a particular processing section due to which the collaboration becomes difficult for service providers to commit fraud.

Because each service is provided by a different supplier, this paradigm promotes availability. There's also data migration, which involves moving data across storage services in order to reduce the control that service providers have over data.

Drawbacks:

1. There is no evidence that this model shows Data Integrity and confidentiality aspects of the security.

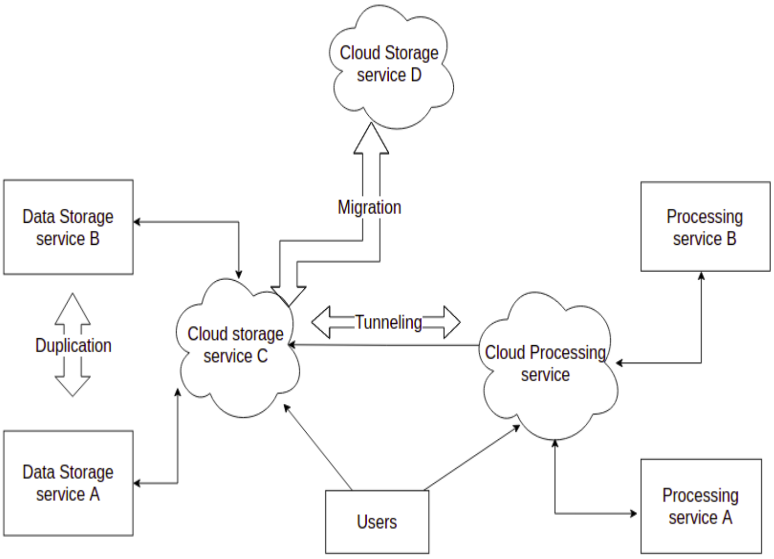

Figure 6: Tunnel Model

This work is licensed under a Creative Commons Attribution 4.0 International License

D. Cryptography Model

In the cryptography model the data that is sent by user into the cloud moves to processing service where data is processed and then that data is sent to data tunneling service.Here cryptography comes into the picture and encryption of the data occurs before sending it to cloud storage service. Cryptography services are here hidden in view of both the service sections.

All user security aspects are covered in this model. Utilization of encrypted data will lead to the failure of many unauthorized disclosures and improve the protection of data.

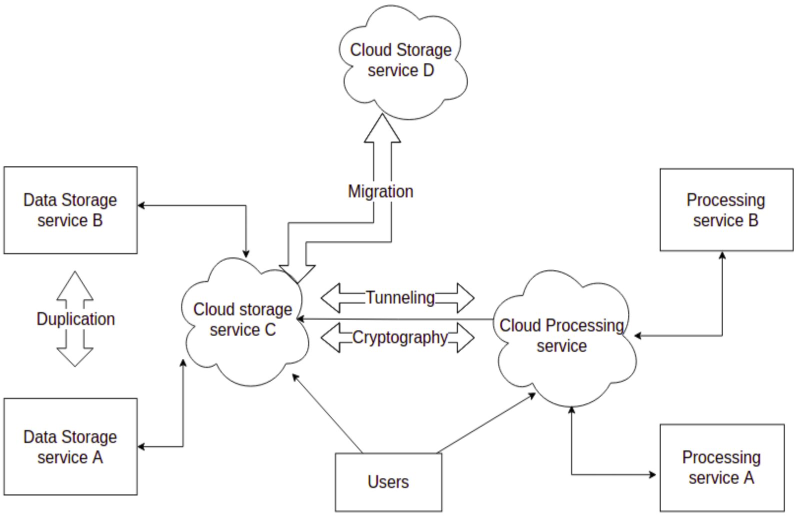

Figure 7: Cryptography Model

E. Collaboration Model

Cloud providers increase their safety in the collaboration model by gathering some of the information into additional systems. At least two cloud systems are incorporated in this model.In case where one storage service is disabled, the other ones come into the picture and perform the operations that users request.Si where one storage device gets hacked the attacker doesn't have the full access to data as some of it is present in the other storage device.The collaborations are made in this model to deliver services safer and need protocols and architectures to communicate transparently between providers of services.

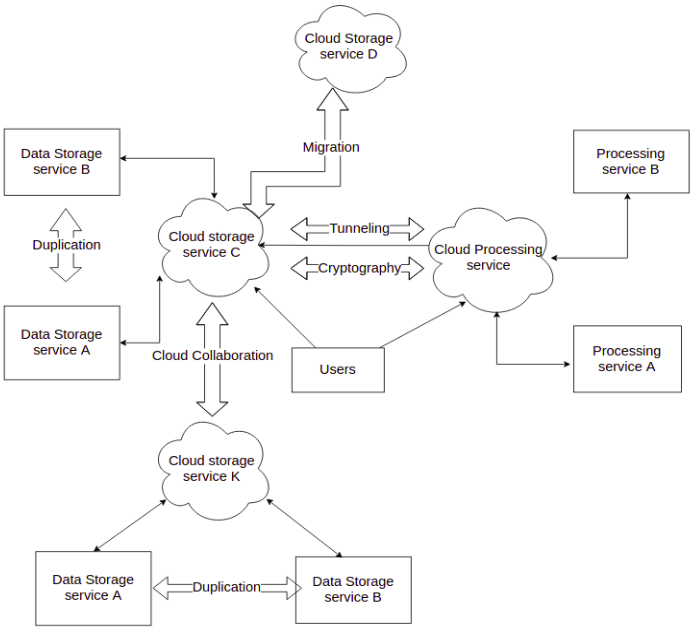

Figure 7: Collaboration Model

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI 10.17148/IJARCCE.2021.105147

V. CONCLUSION

In this paper the various deployment models present and its advantages and disadvantages are discussed.Next, important user concerns are mentioned which are main reasons or issues for users in not adopting cloud computing. Various deployment models are proposed to deal with these user concerns and to enhance the security of the system.

The techniques mentioned are at the level of deployment and not at the level of implementation. The models are based on the inter-cloud interaction and they are user oriented.User awareness of the models is important. This will increase user's confidence in cloud computing.

Future work should focus on the development of cloud-based apps to meet the proposed models and also examination should be done on the cryptographic algorithms that can be incorporated to enhance the security of the system.

REFERENCES

[1] N. R. Putri and M. C. Mganga, "Enhancing Information Security in Cloud Computing Services using SLA Based Metrics," M.S. thesis, Blekinge Institute of Technology, Sweden, 2011.
[2] R. Barga, J. Bernabeu-Auban, D. Gannon and C. Poulain, "Cloud computing architecture and application programming," SIGACT News, vol. 40, no. 2, pp. 94-5, 2009.
[3] J. W. Rittinghouse, and J. F. Ransome. "Cloud Computing Implementation, Management and Security,"by Taylor and Francis Group, LLC. 2010.
[4] G. Zhao, M. G. Jaatun, C. Rong, F. E. Sandnes. "Deployment Models: Towards Eliminating Security Concerns From Cloud Computing," in IEEE, 2010, pp. 189-195.
[5] J. Sen. "Security and privacy issues in cloud computing". Architectures and Protocols for Secure Information Technology Infrastructures journal, 2013.
[6] Hajar Ziglari, Saadiah Yahya
"Deployment Models:Enhancing Security in Cloud Computing Environment" , 2016 22nd Asia-Pacific Conference on Communications (APCC)
[7] L. D. D. Babu, P. V. Krishna, A. M. Zayan and V. Panda, "An Analysis of Security Related Issues in Cloud Computing," In 4th International Conference: Contemporary Computing, 2011, pp. 180-190.

This work is licensed under a Creative Commons Attribution 4.0 International License