ISSN 2277-3061
Volume 16 Number 3
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

A REVIEW ON A SECURITY MECHANISM IN CLOUD ENVIRONMENT

Jaspreet Kaur [(1)], Navdeep Kaler [(2)]
[(1)] Research Scholar, Department of Computer Science & Engineering, LLRIET, Moga
jaspreetcse.dtc@gmail.com
[(2)] Assistant Professor, Department of Computer Science & Engineering, LLRIET, Moga
navdeep.kaler@gmail.com

ABSTRACT

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. As information exchange plays an important role in today's life, information security becomes more important. This paper is focused on the security issues of cloud computing and techniques to overcome the data security issue. Before analyzing the security issues, the definition of cloud computing and brief discussion to under cloud computing is presented. The various components that affect the security of the cloud and the problems faced by cloud service provider have been discussed in this paper.

Keywords

Cloud Computing, Cloud Security, Security issues, OTP, AES, and Hashing

INTRODUCTION

Cloud Computing is one of the biggest technology advancement in recent times. It has taken computing in initial to the next level. Cloud computing is one of the biggest thing in computing in recent time. Cloud computing is a broad solution that delivers IT as a service. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access. The cloud computing flexibility is a function of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet. In the cloud computing, the internet is viewed as a cloud. By the use of cloud computing, the capital and operational costs can be cut.

Figure 1. A Cloud Is Used in Network Diagrams to Depict the Internet

COMPONENTS OF CLOUD COMPUTING

Cloud computing consists of three main components. These components are:

- Clients
- Datacenter
- Distributed servers.

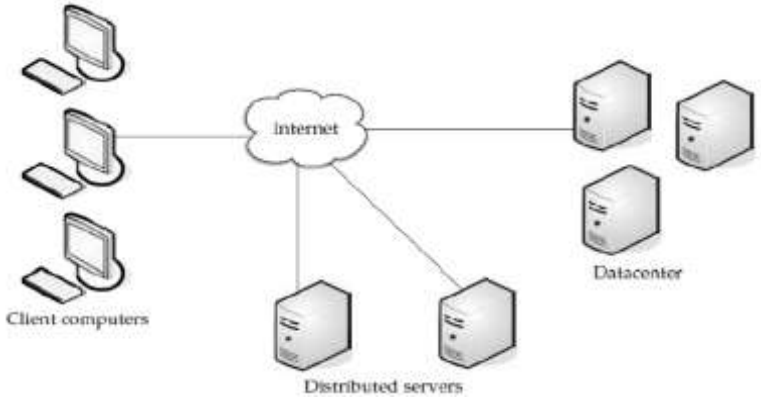

Figure 2. Cloud Computing Components

CLIENTS

In the cloud computing, the information is managed by end users. They interact with the clients to manage information related to clouds. The clients are further classified into three categories:

Mobile Client: the clients can be mobile in nature. It includes windows mobile smart phone, like a Blackberry or I Phone.

Thin: These clients do not do computation work. They only used to display information. These clients don't have the internal memory; the servers do all the work for the clients.

Thick: These clients use different browsers to connect the internet cloud. These browsers include internet explorer, Mozilla Firefox or Google Chrome to connect to the Internet cloud.

DATACENTER

Datacenter is a collection of servers; these servers host the various applications. An end user connects to the datacenter to subscribe different applications. A datacenter is existing at a large distance from the clients. Now days, the concept called virtualization is used to install a software that allow multiple instances of virtual server applications.

DISTRIBUTED SERVERS

Distributed servers are the parts of a cloud computing, these servers are present throughout the Internet. These sever hosts the various applications.

FEATURES OF CLOUD COMPUTING

Scalability: Cloud computing is scalable. That is whenever we need more resources we can add it to the cloud anytime. That is Cloud computing is infinite pool of resources.

Environment friendly: Cloud computing makes efficient use of hardware which helps to reduce energy cost.

Cost efficient: Major feature and advantage of cloud computing is, it is cost efficient. We have to pay that much amount which we used just like electricity bill.

Up to date: We need not to worry about the updates to the software's and hardware's that we are using in the cloud. The provider is responsible for the overall update process of all the components.

Improved performance: Whenever we need some high configuration resources it will be available to the user on its demand.

CLOUD COMPUTING SERVICES

There are various services that are related to cloud computing. As,

Web-based cloud services: These services are related to the functionality of web service. It does not require the fully developed applications. For example, it might include an API for Google Maps.

Software as a Service: In this case the information is divided into various services, and each service is handles by a cloud expert. The example of software as a service is in sales, HR, and ERP.

Platform as a Service: This service is also known as a variant of software as a service. In this case, we can run our own application, but it can be run only on cloud provider's infrastructure.

Utility cloud services: These are virtual storage and server options that organizations can access on demand, even allowing the creation of a virtual data center.

Managed services: This is an oldest iteration of cloud solutions. In this scenario, a cloud provider utilizes an application rather than end-users. For example, it includes the anti-spam services.

Service commerce. These types of cloud solutions are a mix of software as a service and managed services. They provide a hub of services which the end user interacts with.

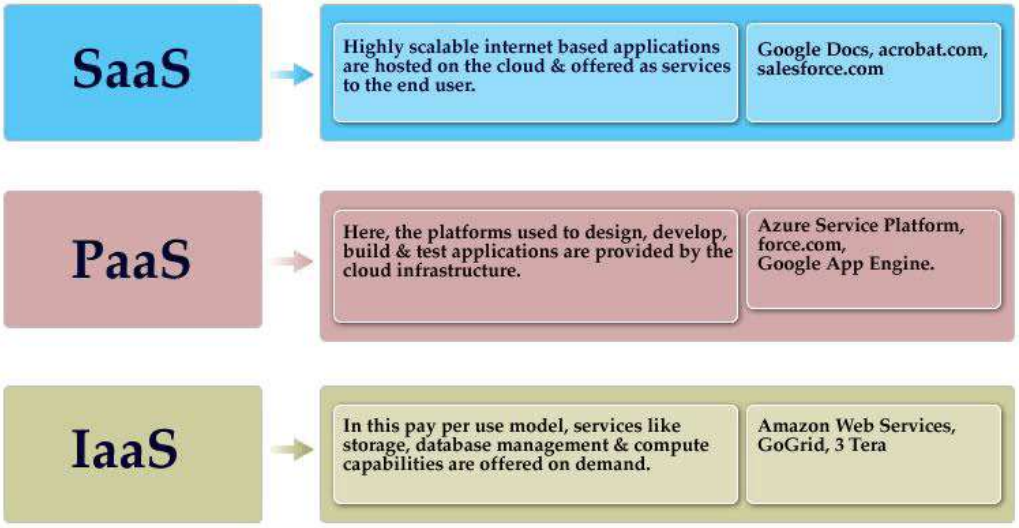

Figure 3. Cloud Computing Models

CLOUD COMPUTING APPLICATIONS

The applications of cloud computing are practically limitless. By the use of right middleware, a cloud computing system could execute all the programs a normal computer could run. There are some basic applications of cloud computing:

- Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer that is linked to the Internet.
- Cloud computing systems would reduce the need for advanced hardware on the client side. There is no need to buy a faster computer with large memory, because the cloud system would take care of those needs for you.
- Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give the access to computer applications for many organizations. The companies do not buy the particular set of software and the software licenses for each employee.
- In the cloud computing, servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on other hardware. It helps for removing the need of physical space on the front end.

CLOUD DEPLOYMENT MODELS

There are different types of clouds that one can subscribe to, depending on the requirement of the client.

PUBLIC CLOUD

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

PRIVATE CLOUD

A private cloud is established for a specific group or organization and limits access to just that group.

HYBRID CLOUD

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized technology that enables data and application portability. Example cloud bursting for load-balancing between clouds.

COMMUNITY CLOUD

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. A community cloud is shared among two or more organizations that have similar cloud requirements Example: security requirements, policy, and compliance considerations. It may be managed by the organizations or a third party.

RELATED WORK

Mohis M et al. (2016) proposes a system which includes a Mediated certificate less encryption which is an advanced encryption scheme that offers more security to the cloud data sharing and a steganography method which enhances the security of data inside the cloud Steganography approach reduces the falsification of unauthorized users. Kunal V. Raipurkar et al. (2016) provides new security architecture with Lightweight Directory Access Protocol and proposed system contribution is a security architecture that provides a flexible security model with Data compression algorithm and two-way encryption algorithm. Cloud computing means distribute computer resources over the network with facilitate of internet. Cloud computing is very powerful concept and proffer some services to the consumers. V.Swathy et al. (2016) plans a new public-key cryptosystem which create constant-size cipher texts such that efficient allocation of decryption rights for any set of cipher texts are achievable. The uniqueness means that one can aggregate any set of secret keys and make them as packed in as a single key, but encircling the power of all the keys being aggregated. Shivangi Sengar et al. (2016) proposes an efficient data model for improving the privacy as well as transparent. The proposed data model is implemented on the different access levels and a cryptographic security is implemented during data access. Additionally, a case study on the governmental organization for distribution of food and fertilizers are reported. R.K.Shyamasundar et al. (2016) presents an approach to building a hybrid cloud that preserves the given security and privacy policy by integrating an RWFM security module into a cloud service manager. An advantage of RWFM is that it provides a uniform solution for securing various kinds of hybrid cloud architectures ranging from the simple pairwise federation to the complex inter clouds, and supporting varying degrees of flexibility in workload placement ranging from a simple static placement to fully dynamic migration. Senam Pandey et al. (2016) works for an access control model of cloud computing in which they added task to the role based access control which enhanced the security of the cloud computing and prevent access to cloud resources from unauthorized user. And also describes the existing access control models and services of cloud computing.

Pooja More et al. (2016) achieves cloud data security by proposing a constant size cipher text key based cryptosystem that uses attribute based aggregate key. In this cryptosystem, to access the data stored over cloud, an aggregate key is shared based on the attributes of a user. Data owner shares an aggregate key only to those users whose attributes gets matched with the security policy. Deepak Singh et al. (2016) proposes a new framework to protect Confidentiality and Integrity of data stored in cloud. In this framework, we use AES, SHA-1, and Station-to-Station Key Agreement protocol. The model proposed here is adapted for thin clients like PDA, mobiles etc. And several technologies have been discussed to make the data safe in cloud storage. Kunal V. Raipurkar et al. (2016) provides new security architecture with Lightweight Directory Access Protocol and proposed system contribution is a security architecture that provides a flexible security model with Data compression algorithm and two way encryption algorithm. Now contemporary year cloud computing has been an up-and-coming computing model in the information technology sectors. It must transmit bulky amount of data to large cloud storage. For safe and sound transmission of critical information in insecure network of cloud computing, encryption of vital information is very important tactic. Shivangi Sengar et al. (2016) proposes an efficient data model for improving the privacy as well as transparency of a data model. The proposed data model is implemented on the different access levels and a cryptographic security is implemented during data access. Additionally, a case study on the governmental organization for distribution of food and fertilizers are reported. The implementation of the proposed security and access control model is provided using JAVA technology. Ahmed Albugmi et al. (2016) discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have security loopholes in them. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might have a security loophole in it.

Aarti Singh et al. (2016) proposes a hybrid two-tier agent based framework which deploys symmetric and asymmetric key algorithms in combination to provide robust security to user data. Further, this mechanism provides data decryption control to user only, thereby eliminating threat of data being misused by cloud service provider. Bin Feng et al. (2016) designed an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support dynamic data operations, which is efficient and has been proven to be secure in the random oracle model. We extended our auditing protocol further to support bidirectional authentication and statistical analysis. In addition, we use a better load distribution strategy, which greatly reduces the computational overhead of the client. Mrinal Kanti Sarkar et al. (2016) proposes a new framework and an Encryption Schemes which encrypt the data and retrieve the data efficiently. The performance evaluation and validation of the proposed model is carried out and the result of performance analysis shown that our architecture is feasible, scalable and efficient. It can provide deferent types of service over the internet. One of the important services is provided by the cloud is storage where users can keep their data as per the requirement. So, it is a challenging issue for the user, as all the data are stored in some inter-connected resource pool but this resource pool is situated over different places of the world.

N.Thillaiarasu et al. (2016) summarizes the security benefits in deploying multiple different clouds in parallel. The frameworks were discussed based on their security and confidentiality measures. In cloud computing the security features still remains a big problem during its deployment. The security threats are under research proposing several techniques for overcoming the threats. Focusing on security issues the cloud computing gives rise to several independent features which paves way for security observations, techniques and frameworks.

Rohan Raj Gupta et al. (2016) proposes an implementation of encryption of user data when it is uploaded to the servers, reduces the cost overhead of encryption as we are not using standalone hardware servers for encryption which waste resources even if they are not in use. Our method will be implementing Docker instances which will be used as an encryption server, which will use resources only when a file is received and after encrypting the file, the docker instance will be shut down, hence reducing the resource usage and reducing the cost altogether. S.Petcy Carolin et al. (2016) proposed\s a

Virtualization and Data Recovery to create a virtual environment and recover the lost data from data servers and agents for providing data security in a cloud environment. A Cloud Manager is used to manage the virtualization and to handle the fault. Erasure code algorithm is used to recover the data which initially separates the data into n parts and then encrypts and stores in data servers. Theodoros Mavroeidakos et al. (2016) defines multilayered security architecture based on defense in depth. In this architecture, the cloud infrastructure is divided into defense zones to achieve better security control. Additionally, intrusion detection system (IDS), honeypots and firewalls are incorporated alongside the defense mechanisms of the cloud infrastructure. In this way, a secure architecture is applied in which the end service is provided uninterrupted, while control over the level of security is maintained.

RESEARCH GAP

In order to avail the benefits of cloud, we must ensure the security of data being transferred between the client and user. Security is the key for the Cloud success, security in the cloud is now the main challenge of cloud computing. Until a few years ago, all the business processes of organizations were on their private infrastructure and, though it was possible to outsource services, it was usually non-critical data/applications on private infrastructures. Now with cloud computing, the story has changed. The traditional network perimeter is broken, and organizations feel they have lost control over their data. New attack vectors have appeared, and the benefit of being accessible from anywhere becomes a big threat. After studying the existing papers, it is analyzed that the existing techniques are not capable of protecting data.

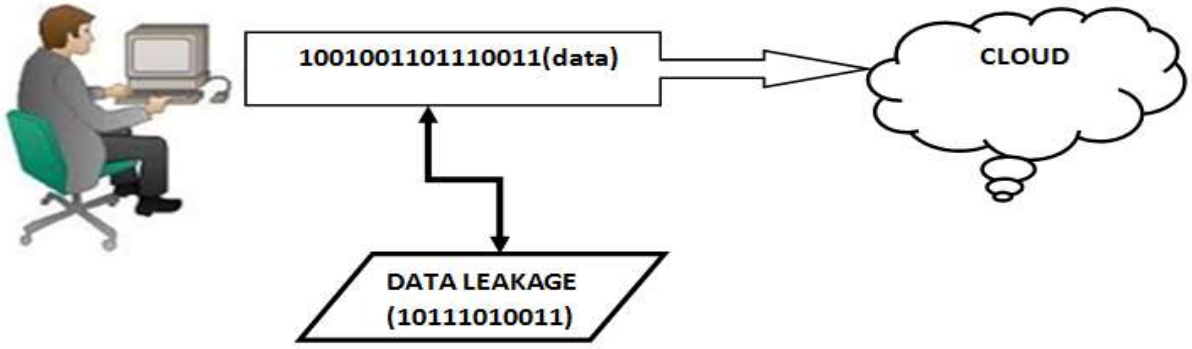

Figure 4. Man-in-the-middle Attack

We will try to enhance Security between the client and cloud accessing the cloud. No doubt, cloud has got multiple benefits but we should not forget that there is a high risk of data getting confidential information getting leaked as shown in figure 3.1

PROBLEM FORMULATION

There are various policies issues and threats in cloud computing technology which include privacy, storage, reliability, security, capacity and more. But most important among these to concern is security and how service provider assures it to maintain. Generally cloud computing has several customers such as ordinary users and enterprises who have different motivations to move to cloud.

Various concerns after analyzing the problems in cloud Computing are:

- Security
- Integrity
- Loss of data
- Third party access

The only way to increase data protection, confidentiality and integrity is to keep in mind that the data is protected during transmission and at rest within the cloud using file-level encryption.

- No secure authentication: In the present work, there is no secure authentication procedure defined. When you log on to your machine and then try to access a resource, say a file server or database, something needs to assure that your username and password are valid. With sensitive data stored in the cloud of the different users, we need a strong authentication mechanism along with OTP. Data breaches because of no/weak authentication.
- No Gateway is defined: The user should not be directly connected to the cloud provider as there is high risk of data getting stolen or hacked by the third-party intruder. There is a requirement of gateway/broker that acts as an intermediate between the cloud provider and the client.
- Weak Encryption Mechanism: In the present work, only one encryption algorithm is chosen i.e. AES for encryption of data at the client's end.
- No Integrity of the client's data is maintained.

CONCLUSION

Cloud computing by itself is in evolving stage and hence the security implications in it aren't complete. It is evident that even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decision to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest comes when the differences between actual cloud security and virtual machine security comes. Research should be center on these gaps and differences and its removal. Main goal of cloud computing is to securely store and transmit the data of the client.

REFERENCES

[1] Mohis M and Devipriya V S, "An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique," IEEE, pp. 1-5, 2016.
[2] Kunal V. Raipurkar and Anil V. Deorankar , "Improve Data Security in Cloud Environment by using LDAP and Two Way Encryption Algorithm," IEEE, pp. 1-4, 2016.
[3] V.Swath, K.Sudha, R.Aruna, C.Sangeetha and R.Janani , "Providing Advanced Security Mechanism for Scalable Data Sharing In Cloud Storage," IEEE, pp. 1-6, 2016.
[4] Shivangi Sengar and Rajesh Kumar Chakrawarti , "Implementation of PDS System with Improved Security and Transparency under Cloud Environment," IEEE, pp. 1-6, 2016.
[5] Mohis M and Devipriya V S, "An improved approach for Enhancing Public Cloud Data Security through Steganographic Technique," IEEE, 2016.
[6] S. Pandey , A. Dwivedi , J. Pant and M. Lohani , "Security Enforcement using TRBAC in Cloud Computing," IEEE, pp. 1232-1238, 2016.
[7] R.K.Shyamasundar, N.V.Narendra Kumar and Muttukrishnan Rajarajan, "Information-Flow Control for Building Security and Privacy Preserving Hybrid Clouds," IEEE, pp. 1410-1417, 2016.
[8] P. More and D G Harkut, "Cloud Data Security using Attribute-based Key Aggregate Cryptosystem," *IEEE,* pp. 855-861, 2016.
[9] D. Singh and Harsh K Verma, "A New Framework for Cloud Storage Confidentiality to Ensure Information Security," *IEEE,* 2016.
[10] Kunal V. Raipurkar and Anil V. Deorankar , "Improve Data Security in Cloud Environment by using LDAP and Two Way Encryption Algorithm," *IEEE,* 2016.
[11] S. Sengar and . R. K. Chakrawarti , "Implementation of PDS System with Improved Security and Transparency under Cloud Environment," *IEEE,* 2016.
[12] A. Albugmi, M. O. Alassafi , . R. Walters and Gary Wills, "Data Security in Cloud Computing," *IEEE,* pp. 55-59, 2016.
[13] A. Singh and M. Malhotra , "Hybrid Two-Tier Framework for Improved Security in Cloud Environment," *IEEE,* pp. 955-960, 2016.
[14] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu and Tie Qiu, "An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing," *IEEE,* pp. 1-13, 2016.
[15] Mrinal Kanti Sarkar and S. Kumar, "A Framework to Ensure Data Storage Security in Cloud Computing," *IEEE,* 2016.
[16] N.Thillaiarasu and ChenthurPandian.S, "Enforcing Security and Privacy over Multi – Cloud Framework Using Assessment Techniques," *IEEE,* 2016.
[17] R. R. Gupta, G. Mishra, S. Katara, A. Agarwal, M. K. Sarkar, R. Das and S. Kumar, "Data Storage Security in Cloud Computing Using Container Clustering," *IEEE,* 2016.
[18] S.Petcy Carolin and M.Somasundaram, "Data Loss Protection And Data Security Using Agents For Cloud Environment," *IEEE,* pp. 1-5, 2016.
[19] T. Mavroeidakos, A. Michalas and Dimitrios D. Vergados , "Security Architecture based on Defense in Depth for Cloud Computing Environment," *IEEE,* 2016.
[20] Deepak H. Sharma, C A. Dhote and Manish M. Potey, "Intelligent Transparent Encryption-Decryption as Security-as-a-Service from Clouds," *IEEE,* pp. 359-362, 2016.
[21] Deepak H. Sharma, C A. Dhote and Manish M. Potey, "Implementing Intrusion Management as Securityas-a-Service from Cloud," *IEEE,* pp. 363-366, 2016.