ENHANCEMENT IN DATA SECURITY USING MULTILAYER CRYPTOGRAPHY

[1]Mr. Akshat Rana, Research Scholar, Department of Electronics Engineering, BMU, Rohtak.
[2]Dr. Anil Dudy, Associate Professor, Department of Electronics Engineering, BMU, Rohtak

Abstract: The use of Cloud services is increasing because cloud services are flexible & scalable services. But the issue of cloud data security is also emerging. When data is transferred from centrally located server storage to different cloud the technical complexities increases. There is always risk to confidentiality & availability of data prior to selecting a cloud vendor or choosing own cloud & cloud service migration. In this paper, we have discussed threats to cloud service & data in case of traditional security system. This paper also discusses the modern security system with system to secure cloud data on multiple layers. This paper explains MD5 and Multiplicative Inverse based Data Encryption Model for security of data during data transmission. Early session timeout is also controlled by reducing packet size. Multilayer security approach is proven efficient to increase the efficiency of data communication along with security.

Keyword: Cloud Computing, Security, MD5 and Multiplicative Inverse, Data Encryption.

INTRODUCTION

The security and risk assessment would include assessing the impact of the combination of risks and attacks on various elements of cloud computing, including; Adaptation of cloud computing, maintenance of confidentiality and protection of individual data, access and reactivation of data. In this way, clear evidence of the most suitable planned orders to support security and reliability in the cloud environment has become the cornerstone of all cloud business contests. Object of the evaluation study " Threats and attacks to security in the cloud computing system: an empirical study is not very appropriate and timely, but it is also an interesting test to update the level of value of information and security of relationships by reliably mitigating security threats in order to reduce “security risks in this new area of cloud computing.” In this review, we investigate and distinguish between indisputable data security and associative security attacks on cloud systems. Existing evaluations show that DoS attacks (DDoS, XDoS, HDoS) and man-in-the-middle attacks are more obvious attacks in cloud partnerships. XSS) are used in all attacks from common and undeniable data security in cloud association collection remains limited to DDoS attacks and is intended to propose intrusion calculations and security reactions against plant- provided malware attacks. In addition, our company is reluctant to collect the cloud towards the completion of the third practical exam.

COMPUTER CLOUD

Cloud computing is an associative innovation that leverages the web and remote specialists who rely on sharing estimates or resources to keep up with data and applications. The capabilities of cloud computing as a "pay-as-you-go" model are one of the most attractive elements. Cloud computing allows you to start sparingly in terms of arithmetic and resource savings and reduce interest in establishing an affiliation with IT. Eliminating and creating machines that run on real hardware and are limited by a hypervisor is a versatile and cost-effective IT perspective. Furthermore, the engagement and total openness of a large amount of "clean" data in different regions, for example in rich regions, can be of immense benefit to researchers and specialists. Cloud computing enables buyers to access online resources from anywhere and at any time over the Internet without having to worry about the specific and actual support or organizational issues of critical assets additionally, cloud computing resources are dynamic and diverse. Cloud computing is free and not at all typical of utility and cross-service computing. Google Apps is the hub of cloud computing; it is accessible to organizations through the program and could be transmitted to a large number of machines on the Internet. Cloud resources can be accessed via the web at anytime from anywhere in the world. Cloud computing is cheaper than other computing models. The included maintenance costs are close to zero, as the network of experts jeopardizes the openness of organizations and customers are free from the help and problems of the market leader in resource machines. In view of this part, cloud computing is commonly known as utility computing or primarily on-demand computing. Flexibility is an essential feature of cloud computing and is perfected through worker virtualization.

Understand how cloud computing technology works

Cloud computing technology works on three different Software Platform Infrastructure (SPI) models and four partnerships (public, private, mutt and neighborhood) Depending on the use or need, the customer can use the cloud and the services in the cloud.

Software Platform Infrastructure (SPI) Models

We currently have three types of organizational models called SPI (Software Platform Infrastructure) models, which are listed below:

SaaS (Software as a Service) - A shipping and shipping scheduling model in which applications are made available to customers as helpers. Clients allow the workplace to access and use an application or organization with which they collaborate in the cloud. The application can run on the customer's computer systems or on the provider's web workers.

The SaaS forces you to significantly establish scale and progress in the effort it facilitated. The least scalability is the most important part of the cloud provider's effort. Basically you use the provider's apps in a link. “Salesforce.com " is a model that uses core data for buyer and support collaboration as part of cloud support and offers Google Apps to large sales organizations, including email and password management.

PaaS (Platform as a Service) : Customers are introduced to the scene by encouraging them to discover your article and cloud applications. IT is at a central point, with extensibility and security elements that must be used by the customer. The main commitment of PaaS is to send the application linked to the client to a cloud. Far from being a programmatic level, it is far from providing help that can be used to bring together higher-level organizations. There are basically two perspectives on PaaS, depending on an organization's provider or customer perspective: to a customer as support. Example: hypervisor virtual machines.

On the other hand, when using PaaS, a synthesis wizard would know them through an application platform interface (API). The client works with the scene through the API and the scene does what is essential to manage and scale everything but a certain level of organization. Virtual machines can be called PaaS instances. In the event that a machine changes substance, for example, all the programming of the section would be stored outside the client and only an API or GUI to plan and transmit the help received. PaaS can force programming to improve and test each time, or it can be a specific district according to leaders. The PaaS business cases consolidate the Google application engine that serves applications on the Google Fabric. PaaS, organizations may, for example, have a strong reason to submit applications to specify or may at least be limited by the capacity that the cloud provider chooses to push.

IaaS (Infrastructure as a Service) - This model is used to provide management, storage, and other core computing resources to customers. The client does not control or manage the basic structure of the cloud, but has an order of the working structure, the main memory and the compute limits as standardized organizations in the binding and transferred to the applications. This requires greater scalability and a lower proportion of security obligations on the part of the cloud provider. The allocation boundary (servers, switches, routers, and miscellaneous systems), storage, rental management, and other important IT resources fit this model.

Distribution models

There are currently four habits through which organizations can be sent in the cloud, the so-called partnership models. These are represented as follows:

PUBLIC: In the public cloud, customers can use web applications and organizations on the Web. Each individual customer has their own resources, which are continually replenished by inviolable resellers / providers. These providers work with different customers on different data networks and handle all aspects of security and provide cloud customers with the tools and framework to function. The customer has no idea how to handle the clouds to make sure the fabric is open. Spacious structure that is available to the individual as a whole and is considered entrusted.

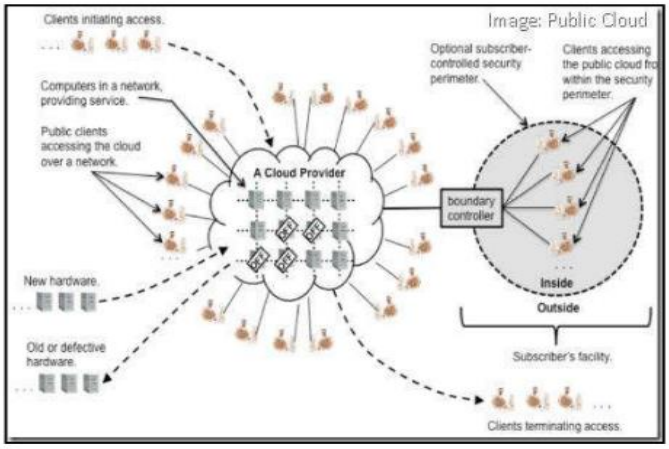

Figure1: Public cloud

PRIVATE: In private clouds, the customer has unlimited control over how the data is managed and what security measures have been taken to plan the data in the cloud. Helping clients are people you trust. The organization's accepted customers are people who are considered a related segment, including agents, project and business plan personnel, insured or leased companies. The private cloud can be deployed on premises (covered) and can be internal (nearby). The local / internal private cloud must be accessible within the affiliation and allow inaccessible customers to pass through. In the reclaimed private cloud, access is simply provided by the approved customer and the cloud is organized in outsourced facilities. As shown in Figures 2 and 3.

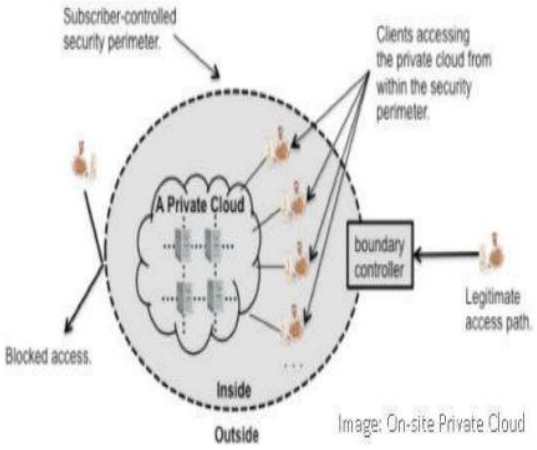

Figure: 2: Local private cloud

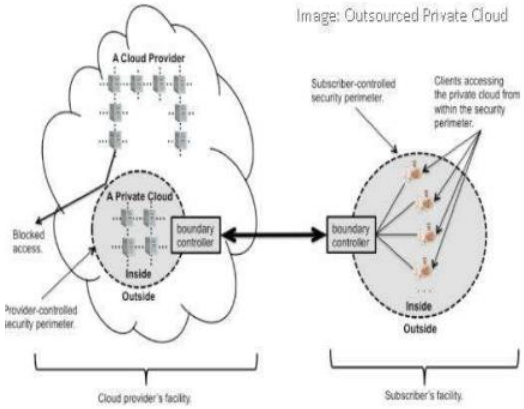

Figure3: Private clouds in outsourcing

Mongrel: It is a combination of no less than two clouds. Hybrid clouds are a combination of public and private clouds within a comparable organization. With the private cloud, customers can save individual data to their private cloud and use the public cloud to process a colossal proportion of readiness requests [10].

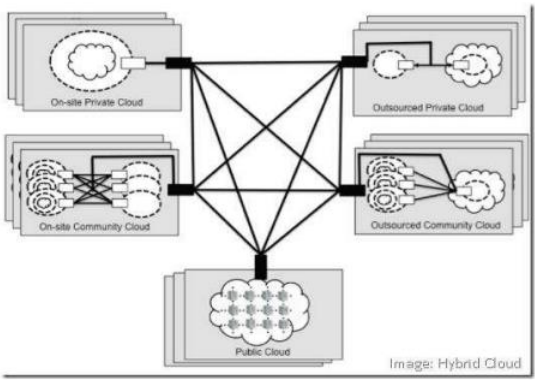

Figure4: Hybrid Clouds

Local Area: This common cloud facility for the express neighborhood. Some affiliations together form and provide a comparable cloud structure along with essential features, functions, and concerns.The cloud neighborhood in a certain degree of financial versatility and vote-based balance. The cloud setup could be tied to a third-party social business broadcaster or one of the local affiliations. The neighborhood will also be redesigned and displayed on the site as shown in the images.

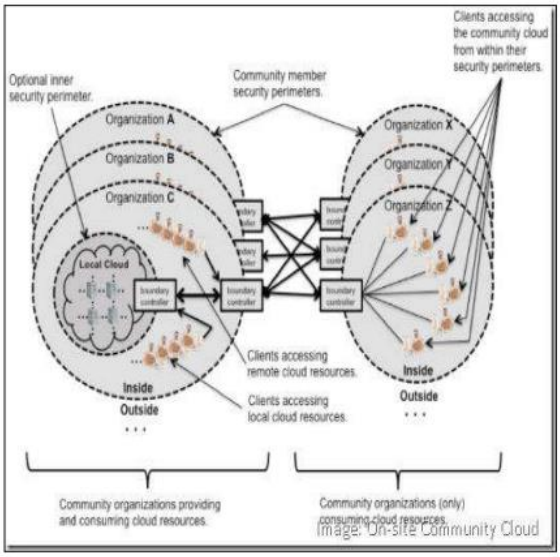

Figure5: Local community cloud

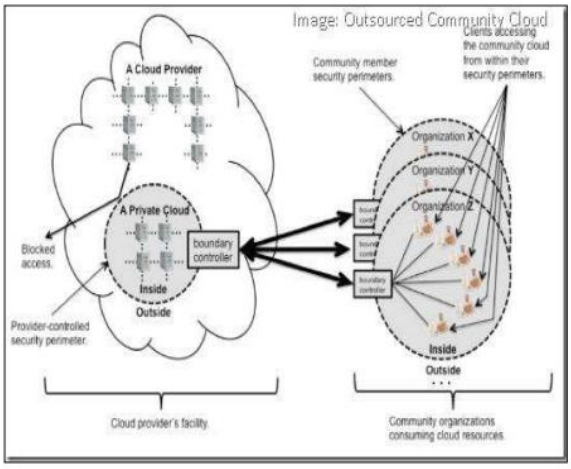

Figure6: Community Cloud in outsourcing

A collection of some associations that have comparable needs and offer a similar foundation can be used with cloud computing. This cloud is more expensive than others, but offers a significant amount of protection, security, or strategic consistency . On-premises cloud computing uses digital ecosystem standards to provide community clouds with a view of the world and provides an elective design for instances of cloud computing use.

Characteristics of cloud computing

Cloud computing is extremely feature-rich, but the key goals of cloud computing coincide with support: Using web-based administrations to support business processes - Cloud computing isn't just for urgent organizations anyway, it's open to the largest organization on the entire internet (it's anything but a project) Show Suite to serve billions of customers around the world). IT management rental on a utility-type site : Cloud computing integrates the rental of IT resources such as hardware, scheduling, and limiting the flow of organizational data on a case-by-case and on-demand basis, such as B. Utility Computing, forerunner of cloud computing; without obsessing over the basic costs and maintenance of cloud

computing.Cloud Computing is a series of existing strategies and subsequent developments, grouped in a different structural perspective, which also offers flexibility, adaptability, commercial status, faster start-up times, reduced organizational costs and without having to talk about the availability of resources for a according to.

The term cloud computing, which describes the revolutionary advancement of many existing advancements and approaches to general IT management, frees up data resources and applications from the central institution and a part used for transmission with the expansion of the allocation of resources, utility and the adaptability model. Cloud computing increases effort, scalability, availability, agility, and offers customers and associations the opportunity to reduce costs. Towards the end of the day, cloud computing describes the use of a multitude of workstations, data and institutions, organization, data, and limited resources; ultimately the right organizations. These parts can be quickly planned, provisioned, executed, and destroyed using a utility model for allocation, performance, and usage.

ISSUES IN SECURITY SYSTEM

In modern area there is need of security for cloud based systems. However the there are several research made in this field. They have used many security mechanisms for data security. But some of them are less efficient. Many systems consume lot of time to process the data during transmission. Thus there is need of more efficient and fast security system for cloud computing.

Third party provides data & infrastructure management in cloud computing so security of cloud is biggest concern.[3] There is a risk in providing sensitive data to cloud service provider. Any security breach could result in customer or business loss so vendors provide protection to accounts.

When data is transferred over cloud network there is always threat from crypto analyst. In order to secure the data and to disable unauthentic user to understand the data there is need of cryptography.

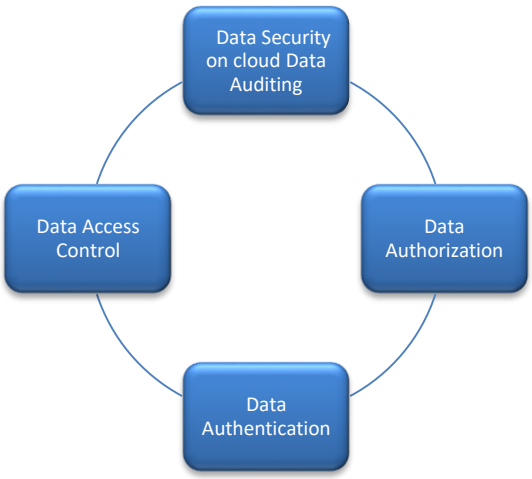

Fig7. Data Security on cloud

Customer cannot switch from one cloud service provider to another quickly so he is dependent on cloud service provider for service. Customer management interface is usually accessible on network in case of various public cloud service providers.

Data security must be considered in cloud because data is frequently transferred over Internet [4]. The basic mechanisms to protect data over cloud are data auditing, data access control, data authentication & data authorization. Due to limitation of existing security mechanisms there was need to develop a new security [3] system. Chance for decryption without authentication should get reduced.

MULTILAYER SECURITY MECHANISM

Such system is providing security to data at many layers. This system is securing content using multiplicative inverse and MD5 approach.

There is need to integrate IP filter-based security in order to prevent attacker from different network. Session layer security would be enhanced by introducing multilayer security mechanism

1. Here IP filter could be used to reject unauthenticated transmission of packets from server to client.
2. Here network security might be enhanced by customizing encryption techniques.
3. Several researchers study loopholes of existing security mechanisms and enhance security of network. Programming of socket server and corresponding client is made to prevent unauthentic access during data transmission.
4. Such type of research makes use of more complex key during encryption and decryption by integration of MD5 and multiplicative inverse cryptographic techniques.

Algorithm on sender side

1. Initialize the port number from receiver for transmission
2. Set the common port number and IP address from sender side
3. Set the file for transmission
4. Perform multiplicative encryption of the compressed data using K.
5. Perform MD5 in order to make data more secure.

Algorithm on receiver side

1. Wait for the data from sender
2. Receive data from sender
3. Apply md5 to decrypt data
4. Perform multiplicative decryption of data using K.
5. Receive the plain data and store in file

CONCLUSION

The paper concludes that such work is capable to reduce the time consumption of data transmission as the size of data gets reduced applying MD5 and Multiplicative Inverse encryption techniques. Due to reduction in size of data, it will take less time for data transmission. In such model user defined port number and IP address are considered to enhance the security of packets at the time of data transmission. Due to reduction in size of packet during data transmission, the probability of error gets reduced. Such mechanisms lead to less error. Moreover the probability of congestion gets reduced and more strong cryptographic mechanism is

developed for secure data transmission.The past region has revealed the closures that emerged from the full investigation. From the information obtained during the evaluation, the expert was able to estimate the possible future degree of the survey. The orientation for the same follows.

- The ordered lightweight encryption chart is evaluated to familiarize you with its advantages over big data. More research is needed from the perspective of map reduction programming with large amounts of data.
- Lightweight cryptography can be enhanced to replicate data components in screened and encrypted data versus homomorphic encryption schemes.
- In the context of the Internet of Things (IoT) as one of the huge data sources with resource-limited teams, it is exciting to see the proposed tools in the IoT use cases united as an enlightening home, a beautiful city and a elegant transportation.

REFERENCES

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On technical security issues in cloud computing," CLOUD 2009 - 2009 IEEE Int. Conf. Cloud Comput., pp. 109–116, 2009.

[2] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.

[3] P. Partheeban and V. Kavitha, "A study with security concerns in service delivery models of cloud computing," Int. J. Appl. Eng. Res., vol. 10, no. 21, pp. 42219–42230, 2015.

[4] Shushing Yu, Cong wang," control fine grained data access in cloud computing,"2010.

[5] V. K. Reddy and L. S. S. Reddy, "Security Architecture of Cloud Computing," Int. J. Eng. Sci. Technol., vol. 3, no. 9, pp. 7149–7155, 2011.

[6] Syam Kumar P and Subramanian R," an effective and safe protocol with the help of ECC and Sobolseries," 2011.

[7] R. Prasad Padhy, M. Ranjan Patra, and S. Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," IRACST -International J. Comput. Sci. Inf. Technol. Secur., vol. 1, no. 2, pp. 136–146, 2011.

[8] Punyada M. Deshmukh ," a system which makes sure the data storage security with the help of a distributed scheme,"2012.

[9] S. Mathew, "Implementation of Cloud Computing in Education - A Revolution," Int. J. Comput. Theory Eng., vol. 4, no. 3, pp. 473–475, 2012.

[10] Santosh Kumar and R. H. Goudar," the designing along with well known platforms of cloud computing," 2012.

[11] Kangchan Lee," Security Threats in Cloud Computing Environments security for Cloud Computing," 2012.

[12] Sajjad Hashemi," the challenges of security, mainly data storage security in a cloud infrastructure," 2013.

[13] Sudhansu Ranjan Lenkaet "RSA encryption and digital signature technique," 2014

[14] swarnalatabollavarapu and Bharat Gupta "data storage security system in cloud computing." 2014

[15] Salah H. Abbdal," issue of making sure the integrity of data," 2014.

[16] Gajender Pal "the introduction of Cloud computing," 2014.

[17] S. Venkata Krishna Kumar1, S.Padmapriya," the offered solution for Coercion has been considered as problem," 2014.

[18] M. Ahmed and M. Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud," Int. J. Netw. Secur. Its Appl., vol. 6, no. 1, pp. 25–36, 2014.

[19] Suraj R. Pardeshi, Vikul J. Pawar "The enhancing information security in cloud computing setting,"2014.

[20] E. Chandanapriya "Effective Data Sharing with the use of Advanced Ring Signature with the help of Forward Security," 2014.

[21] C. Zhang, E. C. Chang, and R. H. C. Yap, "Tagged-mapreduce: A general framework for secure computing with mixed-sensitivity data on hybrid clouds," Proc. - 14th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2014, pp. 31–40, 2014.

[22] M. Computing, G. V. T, J. S. K, P. P. B, and P. S. D, "Improve Security of Data Access in," vol. 4, no. 2, pp. 331–340, 2015.

[23] Karun Handaet "Cloud Computing," 2015.

[24] M. Kaur and H. Singh, "A Review of Cloud Computing Security Issues," Int. J. Educ. Manag. Eng., vol. 5, no. 5, p. 32, 2015.

[25] A. C. Adamuthe, V. D. Salunkhe, S. H. Patil, and G. T. Thampi, "Cloud Computing – A market Perspective and Research Directions," Int. J. Inf. Technol. Comput. Sci., vol. 7, no. 10, pp. 42–53, 2015.

[26] Raj Kumar "cloud computing," 2015.

[27] Burhanul Islam Khan, "the secure, split, merge data sharing in cloud structure," 2015.

[28] Jianghong Wei, Wenfen Liu, Xuexian Hu "The secure Data Sharing in Cloud Computing,"2015.

[29] AL-museelemwaleed, Li Chunlin "The security and secrecy problem transpire in cloud computing,"2016.

[30] Elom Worlanyo, Nidal Hassan Hussein "A survey of cloud computing security challenges and solutions," Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 1, pp. 52–56, 2016.

[31] S. Bulusu and K. Sudia, "A Study on Cloud Computing Security Challenges," Sch. Comput. Blekinge Inst. Technol., pp. 1–137, 2012.

[32] sakshichhabra, Ashutosh Kumar Singh "dynamic data leakage detection model," 2016.

[33] Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, jianshen, huanguozhang "safety, measurement and efficient multi-ownership of data sharing,"2016

[34] Dr.G.M.Nasira, Thangama," the Securing Cloud Database By Data combine Technique," 2016