ISSN:2231-0711
Swati Sharma et al | IJCSET(www.ijcset.net) | 2020 | Volume 10, 1-6

Reducing Insider Attack Using Encryption Algorithms

Swati Sharma[1], Ms. Monika Saini[2]

Department of Computer Science and Engineering
World College of Technology and Management
Guugram,MDU, Haryana, India
swativats07@gmail.com,mona.khushi79@gmail.com

Abstract: Cloud computing has newly developed as an enhanced model for introducing and distributing services over the Internet. It is one of the popular increasing technologies in today's world. It offers on demand services to customers due to this it also known as on-demand computing. It provides the high scalability, high reliability, high performance, easy to access, multisharing and low cost. The important feature is that computing resources are accessible when they are needed. It is a new computing model which provides services for instance Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). It is also called Data outsourcing as a third party provides storage services to user. The cloud data is stored on remote servers and it can be accessed from anywhere and at anytime. This is more cost effective for the uses as there is no need of purchasing costly software and hardware for data storing. When this cloud is made accessible for the customer on pay per use basis, then it is known as public cloud. When customer advances their own applications and executes their specific internal infrastructure then is known as private cloud. Integration of public and private cloud is known as hybrid cloud. However, there has a security issues. In this due to central storage of data it is very important to provide the security. These issues are origin during the distribution of public cloud as in public cloud infrastructure customer is not aware where his data store &how it is stored over the internet. Information protection is one of the most important security issues, as organizations won't deliver its data to remote machines if there is no guaranteed data security from the cloud service providers. Consequently, the future research has to be focus on solving the security and privacy issues.

Keywords: Cloud Computing, Security Issues, SaaS, PaaS, IaaS, Security issues, Deployment models

INTRODUCTION

Cloud computing is one of the most important IT model in the last few years which offered for the companies is reduced time and low costs on the market. It is a new technology for processing and transferring data electronically. Cloud computing signifies a main change in how we store data and run applications. In this Instead of running programs and data on an individual desktop computer, everything is hosted in the cloud. It provides the accessibility of all the documents and application from anywhere, anytime around the world so we can say it is on-demand computing.

Cloud Computing provides unlimited infrastructure to store and execute customer data and program. Cloud can be physical machines or virtual machines. Cloud applications have a large data centres and powerful servers that host Web applications and services. For accessing a cloud application we should have suitable Internet connection. Cloud computing have various benefits which make is more powerful like low maintenance, less IT staff and lesser cost.

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It used in large areas such as banking, e-commerce, retail industry and academics etc. Cloud computing also reduces the risk of capital expenditure for IT companies. In cloud computing all cloud vendors can deliver more efficient management and coordination of cloud resources to get maximized and optimized profit. There are many cloud computing services which are used on daily basis like social networking sites, web based email systems etc. In this Google Driveand Amazon S3 web based cloud services are used.

There are many **Cloud providers** which provide the cloud services these are:-

Google cloud platform:

Google cloud platform is one of the important cloud computing services which are offered by Google and it runs on the same infrastructure that Google uses for its end user products. It has a private cloud that uses for delivering Google Docs. It offers different services like data analysis, machine learning, information storage, email access, document, web application and Google maps etc. It is mainly used for Google search and Youtube.

Amazon web service:

Amazon web service is a cloud computing platform which provides services such as computing platform which provides services such as compute power, database storage and content

delivery. These services are flexible, scalable and reliable. This is no upfront cost and a customer must pay only for what they have used.

Microsoft Azure:

Microsoft azure is a cloud computing service which is used for building, testing and managing the application. It uses virtualization. There is a several amount of virtual machines accessible and each virtual machine can run many operating system. They have invested in cloud computing and provides a variety of cloud-based solutions to individuals and companies. Many organizations deliver services from the cloud.

IBM Cloud Services:

IBM cloud gives services like infrastructure and platform as a service. This cloud association can organize and access its resources for instance storage networking and calculate power with the help of internet. With the help of many tools the customer to describe on industry expertise. Due to high speed of the cloud requirements of customer can be fulfilled. It reduces the difficult problem which faced by large organizations. IBM Cloud computing services are also helpful in retailer, home appliances and manufacturer business. It offers the best services and also fewer prices so it is mostly used.

ARCHITECTURE OF CLOUD COMPUTING

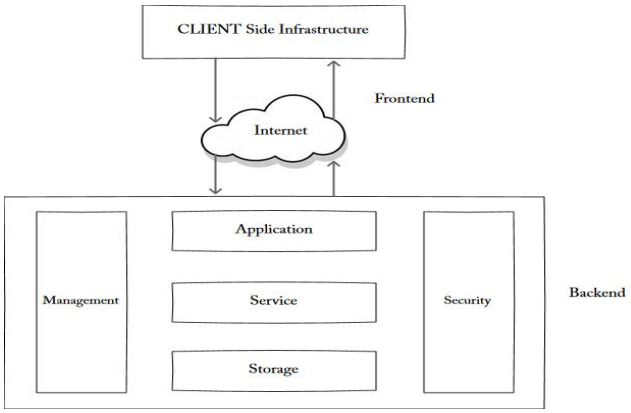

Figure 1: Architecture of Cloud Computing

Front End:

The front end refers to the client part of cloud computing as it is visible for customers or users. It has different interfaces and applications which are necessary for accessing the cloud computing system like Web Browsers (Chrome, Firefox etc).

Back End:

The back end refers to the cloud section because on this side it is used by service provider. It involves huge resources like data storage, virtual machines, deployment models, various servers, etc. It also provides security, traffic management and many other protocols which are required in communication.

Components of Cloud Computing Architecture

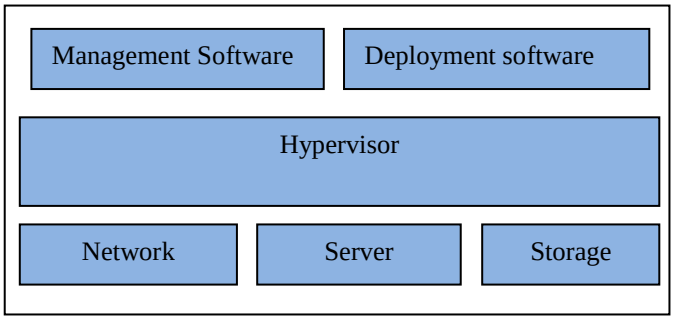

Figure 2: Components of Cloud Computing

Hypervisor:

Hypervisor is a low-level program which acts as a Virtual Machine Monitor. It consists of hardware, software which runs on this virtual machine. It allows managing the guest's operating system and provides a virtual operating platform. It is also known as kernel in the operating system.

Management Software:

Management software includes a huge plan that helps to maintain and configure the infrastructure and increase the performance of cloud. It plays an important role in cloud computing architecture. It has many features like fully accessed, security and on time delivery etc.

Deployment Software:

Deployment means integration of the SaaS, Paas, Iaas. It consists of all configurations and installations of the cloud.
Cloud deployment simply means to initiate the working of the SaaS, PaaS, and IaaS. This initiates the solutions that can access by the users or the customers. This deployment consists of all the mandatory installations and configurations of the cloud. This emerges from the back end and implements before the provisioning occurs

Network:

It plays an important role in cloud infrastructure which allows connecting cloud services over the Internet. Mainly speed of transferring the data depends on the internet connection. In this users are allowed to customize the route and protocols.

Server:

A cloud server works as virtual server that is running in cloud computing .With the help of web it is hosted and delivered by

cloud computing platform. Server offers various services like resource allocation and de-allocation, providing security and monitoring the resources etc. Due to its services it is very secured and stable. It also has a benefit due to its fast up gradation of adding memory and disk space.

Storage

Cloud has several types of storage. It is more reliable due to its storage facility where if any storage resources fail, on that time it can be extracted from another one. It is quickly accessed and also provides a facility that user can remotely accessed with the help of internet.

CLOUD SERVICE MODELS

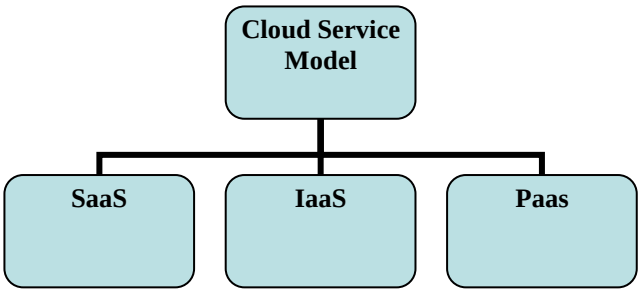

Figure 3: Cloud Service Models

SaaS

SaaS or Software as a Service is a model that allows quickly access cloud-based web applications without installing new infrastructure. It is also known as 'On-Demand Software". The vendor controls and maintains the applications which are run on vendor's cloud, which is accessed by using a web browser. These applications can use them by a paid licensed subscription or for free with limited access. SaaS has no any requirements of any installations or downloads in existing infrastructure so due to this it has no need for installing, maintaining and updating applications on each computer. In this less hardware is required and so due to this it has low cost. On Saas platforms programs can be easily accessible by their employees. All programs in SaaS are fully developed and ready to use. Saas has some problems like lack of control, slow speed, less functionality. Google, Dropbox, Office 365, etc. are the examples of SaaS.

IaaS

IaaS or Infrastructure as a Service gives virtualized term of computing resources above the web hosted by employing a third party. In IaaS model cloud provider can deliver infrastructure components such as networking hardware, storage, servers and operating system. IaaS can provide more storage for any data backup and also high power computing. In this user pay for IaaS on demand instead of purchasing hardware .So due to this it saves cost of maintenance. In this there is no data loss because all data is on the cloud. This model is highly dependent on availability of Internet services. Amazon EC2, IBM, Microsoft Azure, and Google's Compute Engine are some IaaS cloud service providers.

PaaS

Platform as a Service or PaaS is basically a supply an on-demand environment which is generated for developing, testing and organizing the different software applications for user's business. All these resources like storage, networking and servers are managed by platform provider. PaaS is also known as middleware due to its existence between IaaS and SaaS. This model has a major benefit that users are stress free. It is easier to develop as developers only focus on the development without worrying about infrastructure. In this model providers manage operating systems, backups, security etc. In this migration problem is a big issue where difficult to hard to switch PaaS vendors. Google App Engine, Windows Azure, Mosso and SalesForce.com are examples of PaaS. PaaS gives flexible pricing options due to its subscription based features.

CLOUD DEPLOYMENT MODELS

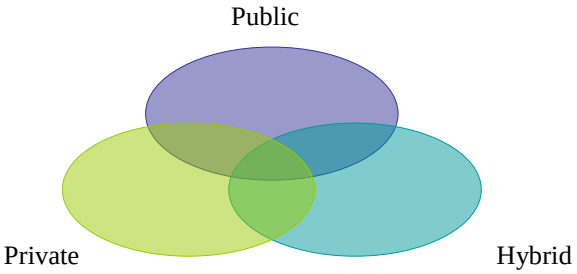

Figure 4: Cloud Deployment Models

Public Cloud

Public cloud is a platform which provides application storage and offered us services over the Internet. The third party manages the public cloud which offers more valuable services like Software-as-a-service (SaaS). These services are available as pay-as you-go billing mode. It is used mainly for small organization which wants to start their business without large investments. It serves several users not a particular customer. Public cloud has many features like low cost, zero maintenance cost, increased reliability and high scalability. Despite of this it has a security problem so it is not appropriate for organizations which have sensitive data. According to usage of capacity cost is decided.

Private Cloud

Private cloud is a cloud infrastructure used by single enterprise or large organizations to manage their data for particular business and not shared by other enterprises. It uses dedicated, private hardware. In private cloud security and

control level is highest as customer information which is very sensitive does not go anywhere. It is remotely located but not shared to others so security and privacy of data is high. In this cost is also reduced if the organization needs to invest in on-premise cloud infrastructure. It provides many operations like disaster and recovery, clustering, maintenance and system monitoring and other services

Hybrid Cloud

Hybrid cloud is a combination of private and public cloud so it is also known as heterogeneous cloud. In this cloud infrastructure is a combination of two or additional clouds that stay distinctive entities but are bound together with the help of standardized technology. Public cloud is used for interaction with customers as well as for running in many applications like emails and private cloud is used for securing the data as well as in data recovery. It has many benefits like cost efficiency, high flexibility, easy transitioning and high security.

SECURITY ISSUES

Data Breach:

In data breaching a hacker collects the whole sensitive information like passwords, financial information, personal information etc. In this another user read all sensitive information.It is occurred when employees may log into cloud systems from their mobile and personal laptops.

Account Hijacking:

In account hijacking hackers or attackers can modify or manipulate the data present on cloud system. There are many ways to hijack accounts like phishing, Password theft and fraud. After accessing the account hackers can reuse passwords for stealing the data and also create false information.

Data Loss:

Data loss is a major issue in which data on cloud services can be permanently lost due to natural disaster, failure of servers and by mistake data erases by cloud service provider etc.

Denial-of-service (DoS):

DoS is a type of security issue where hackers prevents users from accessing their data. In this system can be slow down. This mode of attack utilizes system resources like disk space, power, memory etc. in large quantity to slow down the system as much as necessary that users cannot able to access their data.

Malicious Insiders:

Insider threat occurred from employees in an organization or team who accessed all sensitive data or secret information and misuse it. Detection and prevention of this attack is very difficult job. For instance giving Platform as a service to a number of user or organization can guide to data theft. One more example Facebook if once authorizations are provide to applications they can get all data related to users. So currently problem is to find solution of such type of problem. For this a Zero Trust Security model is an upright solution to resolve this security issue.

FEATURES OF CLOUD COMPUTING

Resources Pooling

In this with the help of a multi-tenant model cloud providers pulled the computing resources to serve multiple consumers with different physical and virtual resources assigned and reassigned that depends on consumer's demand. Normally in this customer has no control or information over the location of the provided resources like storage memory, processing, email services and network bandwidth but may possibly be able to recognize location at advanced level of abstraction.

On-Demand Self-Service

It is the important features of Cloud Computing where user themselves are able to monitor and manage computing capabilities, such as server time and network storage. In this there is no role of any human administrators. There are many cloud service provider who gives these on demand self-service like Microsoft, Amazon web services and Google etc.

Easy Maintenance

In this downtime is very low or many time there is no downtime and the servers are simply maintained. With the help of updating, performance of Cloud Computing comes in a faster way than older ones where bugs are fixed.

Large Network Access

With the help of a device and an internet connection user can upload or download the data of the cloud. All these capabilities are accessible all over the network and accessed by internet.

Security

Security is the best features of cloud computing. With the help of snapshot of stored data may not get lost. Data cannot be hacked or utilized by any unauthorized person because data is stored within storage devices. With the help of any device and internet connection we can access it from anywhere due to quick and reliable storage services.

Availability

Availability means user can accessed the services at anytime

and from anywhere. The capabilities of the Cloud can be customized as per the use and can be extended a lot. The capabilities of the cloud can be modified as needed and can extend a lot. It analyzes the storage usage and allows the user to buy extra storage if needed for a very small amount.

Automatic System

Cloud computing automatically analyzes the data needed and supports a metering capability at some level of services. We can monitor, control, and report the usage. It will provide transparency for the host as well as the customer.

Economical

It is the one-time investment as the company (host) has to buy the storage and a small part of it can be provided to the many companies which save the host from monthly or yearly costs. Only the amount which is spent is on the basic maintenance and a few more expenses which are very less.

Pay as you go

The user has to pay only for the service or the space they have utilized. There is no hidden or extra charge which is to be paid. The service is economical and most of the time some space is allotted for free.
In cloud computing, when users utilize the services on that time they have to pay. In this there is no extra charge.

Measured Service

Cloud computing usage of resources can be analyzed, measured, controlled gives transparency both the user and provider of the utilized service. For controlling and optimized resources usage cloud computing services use a metering capability. In this utilization of resources is analyzed or measured by sustaining charge-per-use capabilities.

ADVANTAGES

Cost efficient

One of the main advantages of Cloud computing is the less cost. Cloud computing offers services to the organization at cheapest rate. The company can save capital costs as well as infrastructure and maintenance cost. It also reduces the operational and administrative costs. .In this customer has only for what they have used so that there is no upfront cost. It is a fallacy that only the large organizations are able to use it. Though, the little startups can also utilize it as it is cost-effective and safe.

Reliability

Cloud computing is extremely reliable due to the secured storage of data and this data cannot be erased. There are numerous copies of the information are made. If any crashes occur in the database the data can be found from the other database.

Manageability

Cloud Computing helps to manage a large amount of things. In this user needs only a device and internet. All the tasks like maintenance job are executed by the central administrations of resources and infrastructure is managed by vendor etc. If any issue occur in Cloud Database or any part it is managed by the host who manages all things which is profitable to the customers.

Data Centralization

In data centralization all the information store in one place so that user can access from any remote places. There are various projects where data stores on a single place and can right to use at anytime and anywhere.

Proper Security

The organizations always choose the highest security level of the data. For that user can use passwords, encryption schemes and a proper audition.

DISADVANTAGES

Internet Connectivity

Cloud Computing requires internet connectivity so without internet connection user won't be able to access the cloud services. Besides, there is no other way to collect the data from the cloud computing.

Lower Bandwidth

Lower bandwidth reduces the benefits of the clouds such that it cannot use appropriately. A satellite connection can lead to quality disruption, due to higher latency or higher bandwidth.

Security Issues

Since Cloud Computing is very secure but still it requires an IT consulting firm's assistance and advice. Neglecting this can lead to the fact that the business will become vulnerable to the hackers and the threats.

Agreements

There are many vendors accessible which have agreements that are invariable. It is one of the cons for the organizations.

Lacks of Support

Sometime cloud computing providers fail to give suitable support to the consumers. Besides, they want consumers to depend totally on FAQs, which can be a tiresome situation.

Variation is Cost

Cloud Computing is a cost-effective choice, but in this cost of software installation is high. Installation can lead to various expensive features which can be non-profitable for future scope.

PROPOSED WORK

In this part a plan is discussed that gives security for user's information on cloud with the help of encryption technique. This proposed research work mainly focuses on security of information from insider theft. Its solution is to use different algorithms for securing the data from insider theft. According to this all data must be in encrypted form so no one use our information in any wrong manner. This technique is effective for security purpose and all cloud service providers must be implementing this proposed research work. In existing model there is a problem that if any insider theft our data then he can easily set a machine using the encryption/decryption algorithm for applying brute force attack on user's information. It takes lot of time but at present time where processing power fast time for decoding can be less. However, in present model insider uses brute force attack for decoding the security code. This proposed research work tries to enhance security. So, this model suggests CSP should use set of algorithms in spite of using single encryption algorithm for all user, but for a user only single encryption algorithm will be used on data and no information regarding the selection of encryption algorithm will be stored in database. In this proposed model user's encryption algorithm will be one from set of encryption algorithm and now if anyone tries to apply brute-force attack on user's data. On that time attackers need to develop a machine for all algorithm which takes more time. If attacker develops a machine for encryption then on that time it takes more time and for this there is a need of high processing power resources which is very costly and not easy to buy it. Second case attacker can develop encryption machine but that will increase time to encrypt algorithm. So, this proposed model proves that this model is strong to improve security from any Internal attack or Internal theft.

OBJECTIVE

The main aim of this research work is to identify and understand the security issues which affect the performance of Cloud Computing and also develop a scheme to improving security from internal theft.

The specific objectives of this research paper are:

- To evaluate different types of security issues or challenges that affect data in cloud storage.
- To analyze the pros and cons of various algorithms used for cloud security implementation.
- To develop a scheme for improving cloud data security with the help of encryption.

CONCLUSION

Cloud provides many benefits to its users but it has various security problems due to its open environment. Cloud must be safe from all the insider threats so this planned model tries to increase security from insider theft. Even though this proposed model is based on Storage as a Service but it can be implementing on any application on cloud (Software as a Service). SaaS is upper layer of service model of cloud and it's the layer which interacts with the costumers directly. On this layer encryption and decryption of data is done. If CSP or private cloud organization work on this proposed model with their software services than they can protect their data from insider theft. If CSP will apply this proposed model with SaaS CSP required to develop a plugin like software. This software is attached with software service on cloud and stores all encryption and decryption algorithms. So if anyone opens file on that time files passes through plugin and get decrypted and when users saved his work and closes file on that time again file passes through that plugin and encrypt the data. After encryption that file stored on cloud.

REFERENCE

[1] P.Jyothi,R.Anuradha, Dr.Y.Vijayalata"Minimizing Internal Data Theft in Cloud Through Disinformation Attacks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013

[2] Kire Jakimoski"Security Techniques for Data Protection in Cloud Computing" International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016)

[3] Prerna,Parul Aggarwal" Cryptography Based Security for Cloud Computing System" International Journal of Advanced Research in Computer Science ,Vol. 8, No. 5, May-June 2017

[4] Shahin Fatima, Shish Ahmad, Shadab Siddiqui"Security Issues In Cloud Computing : A Survey" International Journal of Advanced Research in Computer Science (ISSN: 0976-5697) Volume 9, Special Issue No. 2, April 2018

[5] Shantanu Sarkar, Vimal Kumar Bharadwaj, Priya G" Security Issues and Challenges in Cloud Computing" International Research Journal of Engineering and Technology e-ISSN: 2395 -0056 Volume: 03 Issue: 10 | Oct-2016 , p-ISSN: 2395-0072

[6] Te-Shun Chou"Security threats on cloud computing vulnerabilities"International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013

[7] Vishal R.Pancholi, Dr. Bhadresh P.Patel" Enhancement of Cloud Computing Security with Secure Data Storage using AES" IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010

[8] V. Suresh Babu, Maddali M. V. M. Kumar"An Efficient and Secure Data Storage Operations in Mobile Cloud Computing"© 2018 IJSRSET | Vol. 4| Issue 1| Print ISSN: 2395-1990 | Online ISSN : 2394-4099