Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data Security in Cloud Computing

Tulsi Negi, Swati Chaudhary, Sangita Rautela
CSE Department, Uttaranchal University,
Uttarakhand, India

Abstract— Cloud computing enables on-demand access to shared resources. It lets to use files and applications over the internet. This technology uses both the internet and the central server to maintain data and resources. Apart from benefits from cloud computing, there are several issues associated to it which needs to be addressed. This research paper identifies security challenges for adapting cloud computing and their solutions from real world. This research paper surveyed different types of techniques used to enhance the security of data stored in cloud environment.

Keywords— Data security over cloud, security challenges,.

I. INTRODUCTION

Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. One way to think of cloud computing is to consider your experience with email. Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer; you access it through an internet connection, and you can access it anywhere. If you are on a trip, at work, or down the street getting coffee, you can check your email as long as you have access to the internet. Your email is different than software installed on your computer, such as a word processing program. When you create a document using word processing software, that document stays on the device you used to make it unless you physically move it. An email client is similar to how cloud computing works. Except instead of accessing just your email, you can choose what information you have access to within the cloud.

The National Institute of Standards and Technology defines cloud computing as follows: "*Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models*."

Cloud computing basically provides three different types of service based architectures are SaaS, PaaS, IaaS etc.

SaaS (software as-a-service):- It offers application as a service on the internet.

PaaS (Platform as-a-service):- This is to be used by developers for developing new applications.

IaaS (Infrastructure as-a-service):- It is basically deals by providers to provide features on-demand Utility.

Recent developments in the field of cloud computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing: 1) The transmission of personal sensitive data to the cloud server. 2) The transmission of data from the cloud server to clients' computers. 3) The storage of clients' personal data in cloud servers which are remote server not owned by the clients

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or the resources remain somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure. In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result, security has always been an issue with cloud computing practices. Robustness of security and a secured computing infrastructure is not a one-off effort, it is rather ongoing – this makes it essential to analyze and realize the state-of-the-art of the cloud computing security as a mandatory practice.

II. RELATED WORK

While coming with this paper we have referred the technical paper on Secure Data Access over Cloud Computing and Secure Data Access in Cloud Computing. We also had visited many previous research papers, survey papers, blogs and websites those are related to the data security in cloud computing. [1] Mahmood identifies that the major issues pertaining to data security in the cloud computing environment are:

 Data Location and Data Transmission — the customers may want that data should reside on a specific territory based on data polices and legislations within the certain country. Similarly, cross border transition of data (from one country to another) may lead to potential risks due to varying policies, regulations and legislations.
 Data Availability — the unavailability of data may lead to service outages.
 Data Security — when the data mobility is at high level, then security risks become the major concern, particularly, when data is transferred to another country with a different regulatory framework.

[2] A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.

Cloud computing security is the major concern and has various challenges that need attention. Data security is a highly cited challenge in the cloud computing field. Security in cloud computing is totally based on the cloud service provider, who is responsible for storing data and providing security.

III. PROPOSED WORK

In this section we concentrate and organize information related to cloud security and to facilitate future studies, we identify the main problems in the area and group them into a model composed of seven categories. Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:

A. Data Security

Security provided by cloud service provider might not be highly cost effective when implemented in small companies, but when two or more organizations share a common resource there is a risk of data misuse. In such situation it is required to secure data repositories. Not only the data repositories but also data should be secured in any stage such as storage, transit or process. Since this kind of sharing resources is prevalent in the Cloud Computing scenario, protection of data is important and is the most important challenge among other CC challenges. In shared areas to keep data secure is challenging than protecting in a personal computer. This problem has begun due to the introduction of new paradigm CC. For enhanced security on data repositories it is important to provide better authentication, authorization and access control for data stored on CC in addition to on-demand computing capability. 3 key areas in Data security that CC refers to are-

1) Confidentiality: When enterprise data is stored outside organizational boundaries it needs to be protected from vulnerabilities. To protect data from vulnerabilities, employees must adopt security checks to ensure that their data stays protected from malicious attacks. Few test are used to help organizations to assess and validate, to which extent data is protected from malicious user and they are as follows:

- Cross-site scripting
- Access control weaknesses
- OS and SQL injection flaws
- Cross-site request forgery
- Cookie manipulation
- Hidden field manipulation
- Insecure storage
- Insecure configuration

2) Integrity: There is no common policy that exists for data exchange. To maintain security on client data,thin clients are used where only few resources are possible. Since only few resources are given access user are not suggested to store any personal data such as passwords. Since passwords are not stored on desktops, passwords cannot be stolen by anyone. Integrity of data can be further assured by:

(a). Using some extra features which are like unpublished API's for securing a particular section of data.
(b). Using DHCP and FTP for long time has been rendered as insecure.

3) Availability: Availability is the most problematic issue, where several companies face downtime (i.e., denial of service attack) as a major issue. The availability of a service generally depends on contract signed between client and vendor. Some other points that need to be highlight when it comes to data security:

i. Who has rights over data (i.e., does data still belong to company?)
ii. If there is any other company or organization being involved (i.e., is there involvement of any third party organization).

iii. Customers using CC applications need to check, if the data provided by cloud service providers is carried out in a lawful way or not.
iv. If data protection fails while data is being processed, it could result in administrative, criminal sanctions or civil type of issues (which depends on country controlling data). These issues may occur due to multi transfers of data log between federated cloud providers.
v. Cryptographic algorithm should be maintained well and updated regularly, failing to do so could lead in disclosing personal data.
vi. Data is not completely protected when it is encrypted and stored. When searching for a piece of information again in CC servers care should be taken to retrieve information in a secured process. Traditional searches can disclose data to other companies/individuals. Not only this but also using complex ways to encrypt can also raise issues while retrieving data from storage.

B. Data Security

To prevent leakage of sensitive information while transferring, a strong traffic encryption technique such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) are required. Sensitive data are obtained from enterprises, processed by any service application and stored at the service vendor end. Amazon Web Services (AWS), provide more protection to its users from traditional network based attacks like MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. The assessment tests to find vulnerabilities in security are based on the following:

a. Network penetration and packet analysis
b. Session management weaknesses
c. Insecure SSL trust configuration

C. VPN Network

If an organization is distributed globally and employees a single vendor, then such organization might experience lower transfer rates when sending a file from one side to another side. A solution to this is usage of Virtual SecurityGateway and maintaining multiple vendors, for implementing this usage of some commercial solutions that give customer-controlled security in a cloud is necessary. This helps to establish a bridge over private infrastructure, where control over cloud lies within the organization. It enables confidentially leverage over the cloud for redundancy, scalability and failover during critical transitions, which may lead to scale up grow or scale down to the organization or business. Some of the network attack types in network security are:

Attack methods such as phishing, fraud, Denial of Services (DoS) and account hijacking are used to steal user credentials.

i. Using traditional network based methods such as IPSec proxies encryption and digital signature, key exchange through SSL proxy which are still being used in the cloud are insecure.
ii. Attack types such as key and password cracking, hosting malicious data, botnet command and control, DDOS.
iii. Backdoors, TCP hijacking, social engineering (where the attacker tries to gain private information from user's social behavior), password guessing, trojan horses and malware are some of the network attacks.
iv. Metadata spoofing is another kind of attack where a new system similar to cloud system can be built by analyzing and re engineering from metadata.
v. Account or service hijacking. In addition to these Dos, IP address modifying helps malicious users to hack into accounts .
vi. Some attack types that are specific to IaaS are DDOS, port scanning and IP spoofing
vii. Side channel attacks and incident handling . SQL injection and phishing by service provider.

D. Data Segregation

Another issue in cloud computing is multi-tenancy. Since multi-tenancy allows multiple users to store data on cloud servers using different built-in applications at a time, various users data resides in a common place. This kind of storage shows a possibility for data intrusion. Data can be intruded by using some application or injecting a client code. The user should ensure that data stored in the cloud should be separated from other customer's data. An encryption scheme used should be assessed and certified that they are safe and cloud provider should use only standardized encryption algorithms and protocols. Vulnerabilities with data segregation can be detected using the following test:

- SQL injection flaws
- Data validation
- Insecure storage

Technology used in Data security: Cloud security is becoming a major area of concern when it comes to regulated data. Cloud customer negotiates their data control to the cloud provider, so there is a risk when the data is another compound. The following are some of the techniques that are currently present in clouds.

Data Masking Technology: Data Masking is the replacement of existing sensitive information in databases with information that looks real but is of no use to anyone who might wish to misuse it. In general, the users do not need to see the actual information as long as what they are looking at looks real and is consistent.

Data masking is not the same thing as restricting the visibility of information in databases from people who are not authorized to see it. In that situation, the data is actually present in the database and is simply not visible to the unauthorized. There are many good and justifiable reasons for taking this approach in a system, but adopting a "data is present but hidden" approach to the protection of data.

Using masking technology, when data passes through the information gateway, confidential parts of the data can be deleted or changed before the data are transmitted to an external cloud.

When compared to encryption techniques, data masking represents how sensitive data is secured. Masked data retains the statistical properties, integrity and realism of the original data, thus allowing effective and efficient development, while eliminating the risk of disclosure of sensitive data.

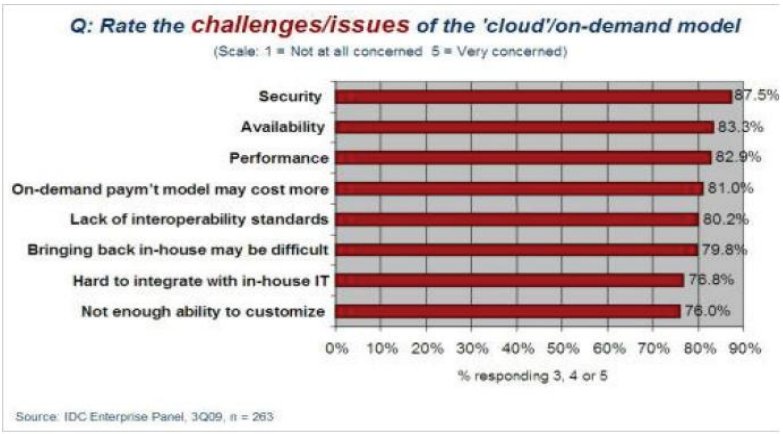
Secure Logic Migration and Execution Technology

For confidential data that cannot be released outside of the company, even formed by concealing certain aspects of the data, by simply defining the security level of data, the information gateway can transfer the cloud-based application to the in-house sandbox[(1)] for execution.

The sandbox will block access to data or networks that lack pre-authorized access, so even applications transferred from the cloud can be safely executed. Moreover, because the execution status of applications is recorded, application providers are able to confirm if there is any inappropriate use of the data.

Data Traceability Technology

The information gateway tracks all information flowing into and out of the cloud, so these flows and their content can be checked. Data traceability technology uses the logs obtained on data traffic as well as the characteristics of the related text to make visible the data used in the cloud. For example, in a joint development project, one can check how textual data collected in the cloud have been used, including whether portions have been copied, thereby enabling any inappropriate usage to be identified.



IV. CONCLUSIONS

In this paper, we presented current issues faced by the Cloud Computing security. The aim of this work is to survey the data security problems in cloud, to solve the security issues faced by the data owners. We consider some data security technologies to resolve the security issues occured in cloud computing. As we noted, one of the most important reason for promoting security in cloud computing is to assure users to use resources in a secure and trusted environment.

This research paper has also discussed current available solutions to overcome some common and major issues. There is need to have better encryption techniques and integrated cloud security framework to make it more dynamic with scalability.

ACKNOWLEDGMENT

I extend my great sense of gratitude and sincere thanks to our research supervisor, Mr. Prashant chaudhary, Asstt. Professor Uttaranchal university, Dehradun, for giving me the opportunity to do research and providing invaluable guidance throughout this research. His dynamism, vision, sincerity and motivation have deeply inspired me. He has taught me the methodology to carry out the research and to present the research works as clearly as possible. It was a great privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me.

It is my priviledge to thank our head of department Dr. Anchit Bijalwan Department of Computer Science for his support and guidance for doing my research work.

I express my sincere thanks to my research guide Mr. Dhanesh Kumar, Asstt. Professor at COER for his valuable suggestion and guidance.

REFERENCES

[1] "The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.Mudili Soujanya, Sarun Kumar,*Personalized IVR system in Contact Center, Department of Computer Science Engineering* International Institute of Information Technology Bhubaneswar, India.

[2] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.
[3] N. Sultan, "Cloud computing for education: A new dawn", International Journal of Information Management , vol. 30, pp109 – 116, .2010.
[4] L. M. Kaufman, Data security in the world of cloud computing, IEEE Security & Privacy, 7 (2009), pp.61-64.
[5] Jianfeng Yang & Zhibin Chen "Cloud computing Research and security issues" in IEEE 2010.
[6] Tackle your client's security issues with cloud computing in 10 steps, http://searchsecuritychannel.techtarget.com/tip/Tackle-your-clients-security-issues-withcloud-computing-in-10-steps.
[7] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST,Germany.
[8] What is cloud computing.Retrived April 6, 2011, available at: http://www.microsoft.com/business/engb/ solutions/Pages/Cloud.aspx.

