International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

DOMAIN DATA SECURITY ON CLOUD

Miss. Sushmita Sukdev Bhoumick

Student, Dept. of Master of Computer Applications , Mumbai University, MET ICS , Maharashtra , Mumbai, India

---

Abstract - *Day by day cloud data security has become more and more important as number of users on cloud is enormously increasing. It is difficult to handle huge data of users. If this data is segregated domain wise then it becomes easy to maintain. As costs for maintaining security are spread among a large number of customers in cloud data centers, cloud operators have been increased and are able to apply far more resources to physical, technical and operational security measures than most corporations or government agencies. Many large service providers across all domains protect data security in cloud computing by operating and maintaining multiple data centers with data replicated across facilities. Security of this data is very important on customer service. Secure software life cycle management are fundamental to the protection of cloud services. Thus the information security of various cloud systems is based on the classical principles of mainly confidentiality, availability and integrity.*

This research paper discusses about the use of securing data on cloud based on different domains. Analysis of data security issues in a cloud environment. It will also discuss about the pros and cons and solutions to them. We will discuss about some important security services, technologies and techniques that include authentication ,encryption and decryption that are provided in Cloud Computing Systems.

Key Words : **Domain , Cloud , Security, Advantages , Data**

1. INTRODUCTION

1.1 Existing System

- User who has data to be stored in cloud and rely only on cloud for data storage and computation can be an enterprise customer or an individual customer.
- Huge single data centers that can get loaded during retrieval of data. Servers can crash as user's data grow in size and importance.
- Huge data storage and availability of duplicate data on a huge amount.
- User to audit the cloud storage for very high communication and cost.

1.2 Proposed System

- Allows users to audit the cloud storage with very lightweight communication and computation cost.
- Domain specific data.
- Faster response time and processing time.
- Supports secure & efficient operations Cost saving, high availability and easy scalability.

1.3 Results

- Data storage on cloud has become important now a day. All the big-big companies are having their data storage on cloud. It defines the growth of the company and increases many customers.

2. WHAT ARE DOMAINS

Domain security can be called as partition of data used for security, notifications and reporting purposes. Data is highly secure within a domain, visibility and creation of data is controlled with security roles in a domain, one can have unlimited nodes and levels[1].

2.1 Data Sharing

Data will be shared to only restricted users. One can choose who can view their data, number of users can be limited. The UI and business rules can be same for all users.

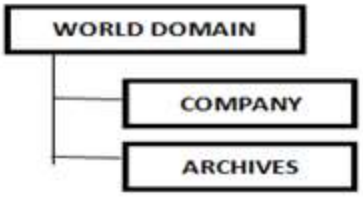

Figure 1: Domain Types

2.2 World Domain And Home Domain

Figure 1 depicts the types of domains. World domain has universal access to all the data across all regions whereas home domain is region specific. The domain value governs access to the users profile but other user's in all the systems. The home domain value defines the default

domains for all the components records are created by different users. It also consists of user experiences. Domains keep data secured.

2.3 What Is Data Security ?

Data security means protecting digital data privacy measures like unauthorized access to databases, websites and also computers such as cyber attack or data breach. It saves corrupting of data. It is a major aspect of IT for organizations. It is also known as computer or information security. It includes disk encryption, data masking, data ensure, backups.

The main data security technology measure is encryption, in this the digital data, software/hardware and hard drives are all encrypted. Authentication is the main method practicing in data security. Users need to provide password, code, biometric data or any unique data to verify the identity before accessing to the system or any data to get full permission. It is also very important for health care records and other medical facilities [2].

CLOUD SECURITY	TRADITIONAL IT SECURITY
Highly and quickly scalable	Slowly scalable
High efficient resource utilization	Lower efficiency
Cost based on usage	Higher in cost
Less time to market	Longer time to market
Data centers provided by third parties	Data centers provided in-house.
Low upfront costs	High upfront costs

Table 1: Cloud Vs Traditional IT Security

3.What Is Domain Wise Data Security?

Distributing data all over in different regions as per customer needs and availabilities. It consists of storage of data centers that are segregated as per different regions on the basics of locals (local languages they use).

This helps in securing data and also data access becomes easy as one can access to only that data that he/she requires. Thus managing and maintaining of that data can be done in a common way as per the domain patterns.

4.What Is Cloud ?

Cloud known as cloud computing is a term that is used for the delivery of hosted services over the internet.it is known as cloud as it refers to applications and services that are offered all over the Internet Cloud computing is an information technology that enables access to shared pools of configurable system resources and a high-level service that can be rapidly provisioned with less amount of management efforts all over the internet.

It is based on sharing of resources to get both economies of scale and coherence. It uses the internet and central remote servers to maintain data. It is an internet based technology that can be used by small businesses and organizations to make use of highly sophisticated computer applications[3].

PHONES,LAPTOPS,SERVERS,DESKTOPS,TABLETS

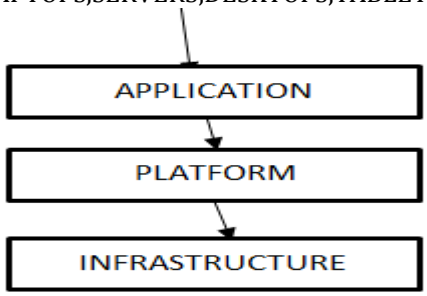

Figure 2: Cloud architecture

- **SERVICE MODELS :**

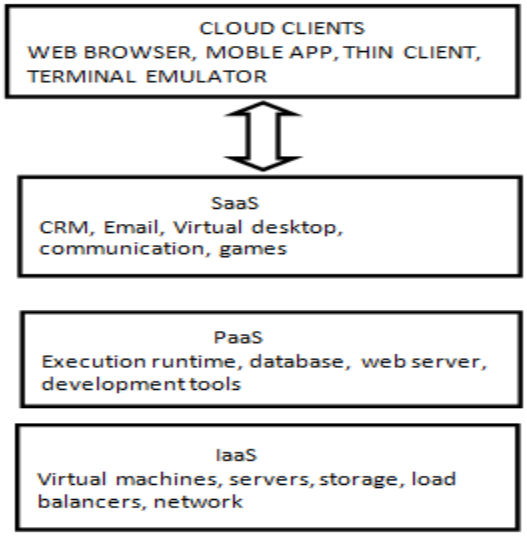

Figure 3: Cloud Service Types

2.4 Cloud Architecture

It consists of multiple cloud components that communicate with each other over a mechanism such as messaging queue. Elastic provision makes use of intelligence in the usage of tight or loose coupling. This architecture of software systems involve the delivery of cloud computing [3].

2.5 Some Encryption Algorithms Used

Various high level encryption algorithm is used to increase protection of privacy. For example, Crypto-shedding is used to delete the keys when they are no more used in the data.

2.6 Attribute-Based Encryption Algorithm

The attribute-based encryption is a basically type of public key encryption. In this encryption the secret key of a user and the cipher text are both dependent upon attributes. Encryption process is based on attributes that are used by different users. The decryption process of cipher text in such systems is possible only if certain basic set of attributes of the user key matches the attributes of the cipher text available.

It consists of two : CP-ABE & KP-ABE.

2.7 Cipher Text-Policy (CP-ABE)

Cipher text-policy i.e. CP-ABE, is an encryption process in this it controls access strategy, as the strategy gets more complex and all the designing and security of the system is highly complex and more difficult.

2.8 KEY-POLICY ABE (KP-ABE)

This encryption uses private keys, the attribute sets are used to explain the encrypted texts and private keys with certain and specified encrypted texts that users need to decrypt.

2.9 SEARCHABLE ENCRYPTION (SE)

Majorly used for secure search, this encryption is cryptographic primitives which provide highly secure functions over the present encrypted data. Search encryption generally builds keywords indexes to securely perform user queries and improve the search efficiency. SE schemes are majorly in two forms: a Secret-key cryptography & Public-key cryptography.

2.10 FULLY HOMOMORPHIC ENCRYPTION (FHE)

FHE focuses with sum and products, allows straightforward computations on the encrypted information, computing sums and product on the encrypted data without the decryption process.

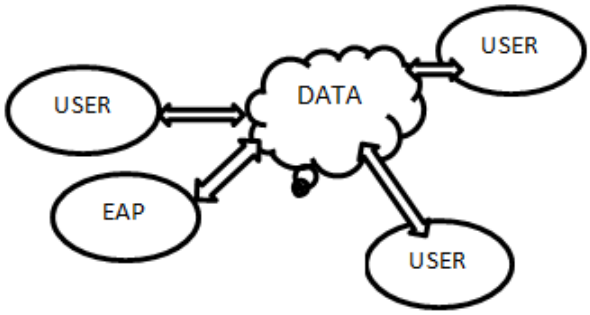

Figure 4 : Domain data security structure

3. SECURITY ASPECT IN CLOUD

As soon as companies get upgraded to cloud their first question is what makes a cloud environment a safer option. One must always take time to review their security posture and what all changes and controls need to be implemented to operate cloud securely. Every cloud customer wants a platform that offers a wide variety of security services to address various requirements and by doing this they can get benefit of all the new features that are available.

3.1 DATA AND RESULTS :

Platforms: Major data services on cloud is offered by amazon's Elastic Compute Cloud (EC2)

- **Amazon Web Services (AWS Cloud Security):**Data security on cloud at AWS is on a priority now-a-days. AWS cloud allows customers to scale and innovate as it maintains a secure environment. AWS cloud customers to scale, maintain and innovate a secure environment. Customers pay for only those services that they use, basically you can organize your own security as per needs at a low cost. Data Security is high in AWS it provides many security capabilities and services to increase high control and privacy of network access. It includes network firewall built into Amazon VPC, connectivity options such as private or connections available from office or on-premises environment.

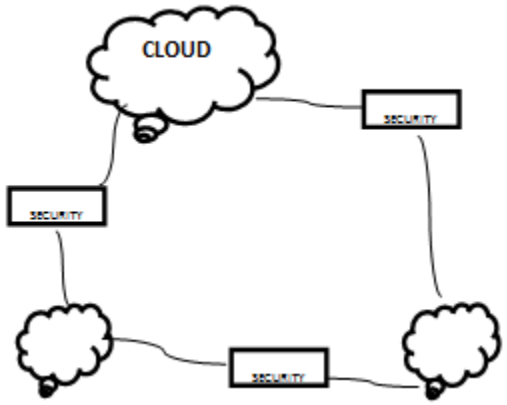

Figure 5: Cloud Architecture

- **Domain Wise Infrastructure :**It spans across 53 available zones within 18 geographical regions around the words and planning 12 more in future. Regions such as US East, US West, Asia Pacific, Canada, China, Europe, South America.

- **Data Privacy : a.** The main focus is on customers, Amazon knows customers care deeply about the privacy and security of data. Amazon does not disclose any information about customers unless there are some legal issues. It gives a prior intimation if there is any need of disclosing data. AWS clients get strong encryption as one of the main security features, an option is provided to manage their own encryption key process.AWS clients have full control over the content present and location where data is stored.

- Microsoft's Azure cloud computing is based on both .NET technology and Microsoft Vista includes both cloud computing and cloud-hosted extension.

- IBM computing on demand / Blue Cloud is an enterprise based cloud computing offering as it is related and build on the same technology that is sold to cloud and can also be cross over between private and public cloud applications.

4. DISCUSSION

- Majorly all the big scale or small scale companies are moving to cloud as they all want to focus on business, use cloud for storing data and be dependent on cloud for security. Thus security on cloud must be a major factor specially on the basis of confidential data. Majorly all the big-big companies have their branches all across the world ,thus their customers and clients are also segregated and all follow different locals and different patterns of data storage facilities as per their needs. Thus big companies prefer to store data on the cloud as per domains i.e. region specific to make it more reliable and available, securing such data is also easy and systematic.

- In 2018, will majorly focus on boarding new IT staff, or advance the skills of existing staff on the basis of a number of key IT trends. Some of these technologies are machine learning and server less computing which are specially related to hybrid and multi-cloud.

- It is flexible a costing level as IT terms must tediously manage and integrate various cloud platforms. Many existing enterprises will be giving cloud based jobs with architects and admin who can build excellent infrastructures and also manage workloads very effectively.

- Invest more on security as it will protect major trust of customers, make customers aware about the storage details and assure them about security. Set up data centers in major part of the worlds and allow proper distribution of data domain wise so that a single data center is not loaded and does not lead to data loss or data center crashing. Train many employees and get upgraded to cloud services as the future relies on cloud. Provide proper courses, knowledge training sessions and also certified training.

5. LATEST TECHNOLOGIES AND TECHNIQUES USED FOR DATA SECURITY IN CLOUD COMPUTING :

Latest Technologies

- Cloud computing has training windows and program in order to address all the challenges, many laboratories that are present have developed new cloud information gateway technology that can flexibly control data, that includes data content, that is transmitted from the inside of a company to a cloud and between multiple clouds. Many companies such as product based companies and service based companies are moving on cloud [3].

- The data gateway also includes many features :

Data Masking Technology

- It is a method of creating a similar but inauthentic version or copy of an organization's data that can be used for various purposes such as training or testing. The purpose is to protect the original data while having a functional substitute for scenarios when the real data is not required.

Secure Logic Migration And Execution Technology

- Mostly all the companies across all domains have secured data that needs to be migrated and also executed at a certain phase in a secured manner.
- Data are highly secured and confidential in big companies ,for confidential data that cannot be released outside of the company, even formed by concealing certain aspects of the data. By defining the security level of data, the information gateway the data can also transfer to the cloud-based application to the in-house sandbox for execution.

Data Traceability technology :

- In data traceability technology, the present information gateway tracks all the information flowing in and out of the cloud, so these flows, the process and their content can be checked.

6. LATEST TECHNIQUES

6.1 Authentication And Identity

- Maintenance of confidentiality, integrity, and availability for data security is a function of correct application and configuration of familiar network, system and application and security mechanisms at various levels in the cloud infrastructure.
- Something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them(such as a fingerprint) [3].

6.2Application Of Encryption For Data In Motion :

- This encryption process is used to assure that if there is a bridge of communication integrity between the two parties so that the data remains confidential.
- Authentication is used to assure that the parties communicating data can be relied on and are who they say they are (no fraud with domains and information).
- The common means of authentication themselves is to employ cryptography in different ways.

6.3 Data Masking

- Data Masking is a technique that is used to protect sensitive information and remove all identifiable and distinguishing characteristics from available data in order to render it anonymous and yet still be operable.
- This technique is highly aimed at reducing the risk of exposing sensitive information majorly used to protect data [4].

7. ADVANTAGES AND DISADVANTAGE

Advantages

- Conducting training and awareness for all system users.
- Domain wise segregation helps faster access to data and easy to maintain as per customer requirements.
- Data segregated by domains follow various locals(local languages as per region to which domain belongs).
- Identifying and authenticating users before granting access.
- Prevent or restrict external attacks.
- Determine the root cause of cyber attacks.
- Reduces the exposure of sensitive data. Simplifies security auditing and testing.
- Enables automated security management. Improves redundancy and disaster recovery.
- Access to highly qualified IT security personnel. Prevent viruses and malware infection.
- Encrypt sensitive or confidential information assets whenever feasible [5].

Disadvantages

- Though cloud provides 100 % data security still other clients feel insecure not Knowing which other client also has the same measures in place [5].

Solution

- Use different encryption keys for each individual client, however it is wholly dependent on the service providers.

- Some businesses take unprecedented risk in storing their critical information on an infrastructure that has not proven to be reliable.
- Data that is unavailable for extended periods of time can be as crippling to an enterprise as data that is compromised.
- Sometimes in certain domains cloud storage security has lack of transparency in the cloud and the users only have the assurance of storage providers as guarantees of security.
- If you have no internet access you cannot access your data and accessing from an insecure network can be risky [5].

8. CONCLUSION :

Future of computing depends on cloud based services. Cloud is the next big way of looking for data storage and security. In order to avoid loss of data and crashing of data the cloud service providers make domain wise data centers that can help users to get secure and reliable data and also be aware about the location where their data centers are stored. Highly recommended and must be expanded on a large scale.

REFERENCES :

[1] The Domain Tools Report, 2016 Edition," The Distribution Of Malicious Domains ",The_DomainTools_Report_Distribution_Malicious_Domain.pdf , Domain Tools

[2] Computer Science Department, Purdue Unwers~ty, West Lafayette, Indiana 47907,"Data Security" Dorothy E. Denning and Peter J. Dennin ,Computing Surveys, VoL 11, No. 3, September 1979

[3] Alexa Huth and James Cebula, “The Basics of Cloud Computing, Produced for an US-CERT,2011 Carnegie Mellon University.

[4] Priya Dhir, Sushil Garg, “Survey on Cloud Computing and Data Masking Techniques”, International Journal of Innovations & Advancement in Computer Science, ISSN 2347 – 8616,Volume 6, Issue 4,April 2017.

[5] Anca Apostu, Florina Puican,Geanina Ularu, George Suciu, Gyorgy Todoran,” Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud“,,ISBN: 978-1-61804-179-1,Recent Advances in Applied Computer Science and Digital Services .