ISSN:0975 -3583,0976-2833 VOL12, ISSUE 02, 2021

DATA SECURITY IN CLOUD COMPUTING

Preeti chaudhary,
Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University,
Dehradun, Uttarakhand India 248002

DOI: 10.48047/jcdr.2021.12.02.91

Abstract:- The term "cloud computing" is currently being thrown around as a buzzword in the industry. Confidentiality, Integrity, Availability, Credibility, and Privacy are critical considerations for both Cloud Providers and Cloud Customers further. The aspect of security in cloud computing is one that is quite vital and crucial, despite the fact that it is coupled with a great deal of difficulty and disadvantage. It is the responsibility of both the cloud service provider and the cloud service customer to ensure that the cloud is sufficiently protected from any and all external threats. This will ensure that the consumer does not suffer any adverse impacts, such as the loss of knowledge or the theft of data, as a result of the transaction. There is also an opportunity in which a malicious user will enter the cloud by masquerading as a normal user, thereby infecting the entirety of the cloud and affecting a huge number of customers who are sharing the infected cloud. This vulnerability can be exploited by an attacker. This vulnerability can be exploited. During this, we are going to talk about the best technique to protect the information from being accessed by unauthorized users and maintain the information's integrity for the users.

Keywords: Data Integrity, Cloud Computing, Steganography Confidentiality, AES,

1. INTRODUCTION

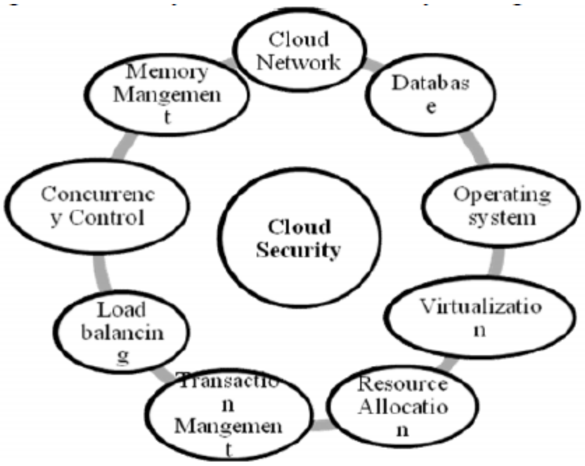
The general understanding of "cloud computing" is always being refined, and the vocabulary and ideas that are used to characterize it sometimes require elaboration. Press coverage might not be specific or might not completely capture the extent of what cloud computing entails or represents. For example, coverage might focus on how companies are making their solutions available within the "cloud" or how "cloud computing" is the way forward, but it might not examine the characteristics, models, and services involved in understanding what cloud computing is and what it will become.

From initial thought building to current actual readying, cloud computing is growing additional and additional mature. today several organizations, particularly little and Medium Business (SMB) enterprises, square measure more and more realizing the advantages by putt their applications and knowledge into the cloud. The adoption of cloud computing could result in gains in potency and effectiveness in developing and readying and save the price in getting and maintaining the infrastructure

In order to facilitate the user's access to the information that they require at a more rapid pace, the architecture of cloud computing calls for many cloud components to communicate with one another regarding the various types of information that they are storing. When discussing cloud computing, much of the attention is focused on the front end as well as the side. The user who requires the information is considered to be the frontend, while the many information storage devices and servers that comprise the cloud are considered to be the backend. There are three distinct types of cloud, each designated by the function that they serve. There are three types of clouds: private clouds, public clouds, and hybrid clouds. A single company controls the data stored in a non-public cloud, while multiple users contribute to the storage of public clouds. The non-public cloud offers superior management as well as a great deal of adaptability. The majority of businesses nowadays make use of something called a hybrid cloud, which is essentially a blend of private clouds and public clouds. The advantages of cloud computing are quite enticing, but there is no such thing as a perfect solution. When it comes to security, the cloud has a number of concerns, mainly with stealing information, losing information, and protecting users' privacy. The characteristics that have an effect on the protection of the cloud, as well as the challenges that are faced by both the cloud service provider and the cloud service client, such as privacy concerns, infected applications, and security issues.

1.1 Parameters affecting cloud security

Computing in the cloud encompasses a wide variety of various technologies, such as networks, concurrent control, database management systems, operating systems, virtualization, resource programming, load leveling, and memory management. As a direct consequence of this, cloud computing is related with a wide variety of various security concerns.



1.2 Security Issues faced by Cloud computing

As of right now, at least some of the operations of more than 70 percent of the world's businesses are carried out on the cloud, as stated by the Cloud Security Alliance (CSA). The fact that 70 percent of businesses use cloud computing is not a huge surprise considering the benefits it offers, which include cheaper fixed pricing, increased flexibility, automatic computer code changes, accumulated collaboration, and the freedom to perform calculations from any location. However, there are still some concerns regarding the cloud's safety. Recent findings from a study titled "Cloud Security Spotlight Report" indicated that "90% of companies area unit terribly or moderately involved regarding public cloud security." These problems cover a wide range, from the potential for vulnerability and account takeovers to the presence of hostile insiders and comprehensive information leaks. Even though the use of cloud computing have ushered in a new age of distributing and keeping information, many companies are still cautious to make the shift or create the transition without a transparent security arrangement in place. This is because cloud computing services rely on a network of remote servers to store and retrieve data. We are going to show you a huge image that contains a printout of the top four problems that you need to keep in mind regarding the security of cloud-based services.

1.2.1. Data Breaches

Despite the fact that data breaches of various types have been around for years, cloud computing and related services are still relatively new. The question that needs to be answered is, "Given that sensitive information is stored in the cloud rather than on premise, is the cloud inherently less safe?" According to the findings of a research called "Man in the Cloud Attack" that was carried out by the Ponemon Institute, more than fifty percent of the IT and security professionals surveyed believed that their organization's security procedures to defend information stored on cloud services were inadequate. For the purpose of determining whether or not that belief is substantiated by real evidence, this study looked at 9 different scenarios in which a knowledge breach had taken place. Following an exhaustive analysis of all potential scenarios, the paper concluded that organizations that store data in the cloud are exposed to a risk that is three times greater than that of organizations that do not make use of cloud storage. The obvious conclusion to reach is that the cloud possesses a distinct collection of qualities that make it a significant amount more susceptible.

1.2.2. Hijacking of Accounts

Account hijacking has been made significantly more difficult as a result of the expansion and use of cloud computing in a number of different businesses. Attackers presently have the ability to utilize your (or your workers') login details in order to gain remote access to sensitive information that is stored on the cloud. Attackers will also falsify and modify data in order to gain access to the cloud using credentials that have been hijacked. Other methods of hijacking include scripting flaws and repeated passwords, both of which enable attackers to take credentials easily and frequently without being detected. In April of 2010, Amazon discovered and patched an issue involving cross-site scripting that attacked customer credentials in addition. Phishing, keylogging, and buffer overflows are all forms of attacks that are very similar to one another. However, the most significant new risk concerns the theft of user tokens, which cloud services employ to verify individual devices without requiring users to check in. This type of attack is known as a "person in the cloud attack."

1.2,3. Insider Threat

Although it may seem unlikely that an attack will come from within your firm, the threat posed by corporate executives will still be there. Staff members will exploit their permitted access to an organization's stored in the cloud services in attempt to access or misuse sensitive information such as client accounts, financial forms, and other types of private data. This behavior will occur since cloud-based services are convenient and easy to use. Furthermore, it is not necessary for these insiders to be coerced into harboring ill will toward the organization. The misuse of data as a result of malicious intent, accidents, or malware was identified as one of the top threats to corporate executives in a survey titled "Inside Track on corporate Executive Threats" conducted by Imperva. The research also looked at four best practices that companies may follow in order to develop a secure strategy. These best practices include prioritizing efforts, controlling access, deploying technology, and business alliances.

1.2.4. Malware Injection

Malware injections are scripts or programs that are inserted into cloud services that act as "valid instances" and run as SaaS to cloud servers. These services are referred to as "valid instances." This provides evidence that malicious malware is intentionally inserted into cloud services, and when it does so, it is misunderstood as being a component of the machine code or service which is operating among the cloud servers immediately. Malicious actors will begin to eavesdrop as soon as the AN injection is no longer active, and as a result, the cloud will begin to function in tandem with it. This will result in the security of sensitive data being compromised, and information will be stolen. A report authored by researchers at East Carolina University titled Security Threats On Cloud Computing Vulnerabilities examines the risks posed by malware injections on cloud computing and notes that "malware injection attack has become a significant security concern in cloud computing systems."

2. EXISTING WORK

Data security and privacy concerns stand as the primary obstacles in the path toward the widespread adoption of cloud computing. Before there is sufficient trust established between customers and cloud service providers, no company will be able to upload any of its information or data to the cloud. In this study, a survey of several strategies pertaining to data security and privacy was carried out. These techniques concentrate on the storage and use of information within the cloud, and their purpose is to provide information protection within the surroundings of cloud computing so that cloud service providers and customers can have trust in one another. In order to construct that trust, it is necessary to supply goodness, confidentiality, and integrity, as well as convenience. Therefore, throughout the course of this paper, we will be supplying.

Confidentiality:

Maintaining confidentiality by authenticating users through the generation of one-time passwords (random numbers) and performing validity checks on users.

Integrity:

Integrity was maintained by putting the password-protected information in a cloud service provider (Drop Box), and steganography was utilized for hiding the most sensitive data, such as passwords. The usual multimedia files were not affected.

Availability:

Connecting to the internet enables users to access these services whenever and wherever they may be required.

3. PRESENT WORK

Cloud computing as well as storage solutions give end users and organizations a choice of options for storing and processing their data in the data centers of third parties. These possibilities are provided by cloud computing and storage providers. When utilizing the Cloud, businesses often make use of a wide number of service models, including as SaaS, PaaS, and IaaS, as well as preparation types, such as Private, Public, Hybrid, and Community models. However, these challenges can be fractured down into two broad categories: security problems encountered by cloud suppliers (organizations which offer software- as-a-service, platform- as-a-service, or infrastructure that is provided as via the cloud), as well as safety complications encountered by their customers (companies or businesses which host applications or store knowledge on the cloud). There are a variety concerning safety issues and concerns associated with cloud computing. The obligation is shared between the user and the provider; however, the provider is responsible for ensuring that their infrastructure is safe and that their client's knowledge and application are secured, while the user is responsible for taking precautions to strengthen their application and making use of strong passwords and other authentication methods.

In Cloud Computing there are three major potential threats

1. Security (for the stored data)

2. Privacy (from the Unauthorized Users)

3. Trust (Data Integrity)

3.1 Data Security and Privacy

Data is stored within the cloud and is accessible by several tenants at the same time. The information location is movable, which means that it is capable of moving from one area to another. Users of cloud storage may forget where their data is stored or who has seen their information, which could lead to security breaches. The fact that the counsel is kept separate from its owner makes it more susceptible to attack. This gives rise to some very significant concerns regarding the protection of the user's knowledge.

3.2 Identity and Access Management

The information that is stored in the cloud is dispersed among a number of different sites; in other words, the cloud provides a mobile storage solution for its data. The user of the cloud service might or might not keep track of where his data is stored. Due to the multi-tenant nature of the cloud, the user of the cloud may be required to sign in using a variety of user credentials while accessing different service providers. This provides a possible risk to the information because someone else could claim to be the original owner in the event that the credentials are lost or disclosed outside the system. In order to draw a significant number of data transfers to the cloud, a cloud environment needs to have an identity and access management system that is both reliable and robust.

3.3 projected System

In this article, we are going to look at a variety of different security methods and issues that pertain to the protection of information storage and personal privacy inside an environment that utilizes cloud computing. The procedures that are used in cloud computing with regard to information security, including information integrity, confidentiality, and portability.

3.3.1 Information Integrity

The maintenance of high data integrity is one of the most important aspects of any data management system. In general, the term "data integrity" refers to the process of protecting information from being altered, deleted, or fabricated without authorization. It is possible to protect valuable information and services from being misappropriated, embezzled, or stolen by managing the admittance of entities and their rights to certain corporate resources. The dissemination of information is controlled by the use of authorization. It is the procedure by which a system determines what level of access a specific authentic user ought to demand in order to safeguard the resources that are controlled by the system. Authentication is the method by which a user proves that they are who they say they are. In the context of cloud computing, "maintaining data integrity" refers to the process of ensuring that information is not destroyed, deleted, or otherwise modified in any way by users who are not authorized to access it. The provision of cloud computing services, such as SaaS, PaaS, and IaaS, is dependent on maintaining the information's integrity. The cloud computing environment often offers processing services in addition to the storing of large-scaled information.

3.3.2 Information Confidentiality

For customers to successfully keep their non-public or secret information within the cloud, data confidentiality is an absolute necessity. Several methods of identification and access management are utilized in order to guarantee the confidentiality of the information. The issues of data security, authentication, and access management that arise in cloud computing may be able to be self-addressed by enhancing the responsibleness and character of the cloud. It is extremely risky for users to put their sensitive information directly in cloud storage due to the fact that consumers do not trust cloud suppliers and it is almost impossible for cloud storage service suppliers to eliminate potential corporate executive threat. Simple encoding is helpless in the face of the key management problem and is unable to fulfill complex requirements such as querying, simultaneous changes, and fine-grained authorization.

4. DESCRIPTION

Authentication and maintaining the integrity of the data are our primary concerns at the moment. The concept of integrity refers to the safeguarding of information against unlawful additions, deletions, and modifications. The term "authentication" implies limiting access to only those users who have been granted privileges.

- We generate random numbers (RN) to authenticate users as part of our authorization process.
- The RN will be delivered to the individual's mobile phone number that was provided at the time of their Registration.
- After the user has entered the code (RN), they will be granted permission to access the information, make changes to the information, and feature information after it has been modified.
- The user will be considered an unauthorized user if they enter the code incorrectly, at which point they will not be able to access the information.
- Users will save transmission information in the cloud storage provided by the cloud service provider, also known as drop box.
- The users' extremely sensitive information will be hidden via steganography and stored in a number of different, highly secure methods.
- The information that is being transmitted will first be encrypted before being transferred to the cloud service provider.
- While the user is in the process of receiving the communication from drop box, it will then be decrypted and made available to them.
- Using this strategy, the information will be protected to a much greater extent and will not be accessible to other users in an unconcealed manner.

4.1 EXISTING TECHNOLOGIES

The process of concealing data within an image is referred to as steganography. It is common practice to employ a variety of steganography methods in order to conceal information. One of these methods, known as image steganography and also known as a

4.1.1 LSB –2 STEGANOGRAPHY

In LSB-2 Steganography the data embedding process is slightly different. It alters the 2nd bit from

right for all pixels [7]. The algorithm is as follows:

Step1: Convert the data from decimal to binary.

Step 2: Read Cover image.

Step 3: Convert the Cover Image from decimal to binary.

Step 4: Break the byte to be hidden into bits.

Step 5: Take first 8 byte of original data from the Cover Image.

Step 6: Replace the least significant bit by one bit of the data to be hidden.

First byte of original information from the Cover Image:

E.g.:- 1 1 0 1 1 0 0 0

First bit of the data to be hidden: 1

Replace the least significant bit

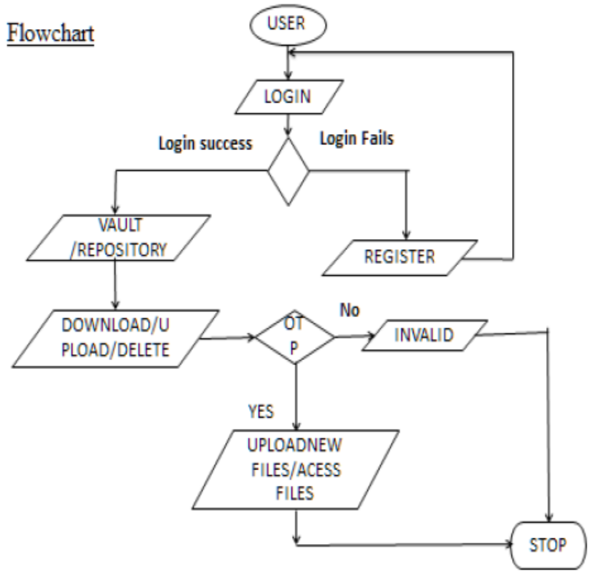
1	1	0	1	1	0	0	0

↓

1	1	0	1	1	0	1	0

Step 7: Continue the step 6 for all pixels.

4.1.2. FLOWCHART



5. AES ALGORITHM

In this section, we will be proposing a framework that will involve the encoding of files in order to provide security for the data. The AES encryption algorithm will be used to secure any files that are stored on the portable device. The user may even transmit and see any of the encrypted data that were previously submitted to the system.

A. AES formula

The National Institute of Standards and Technology (NIST) has indicated that the Advanced Encryption Standard, also known as AES, might be a symmetric-key block cipher. The criteria specified by the agency for making selections are as follows.

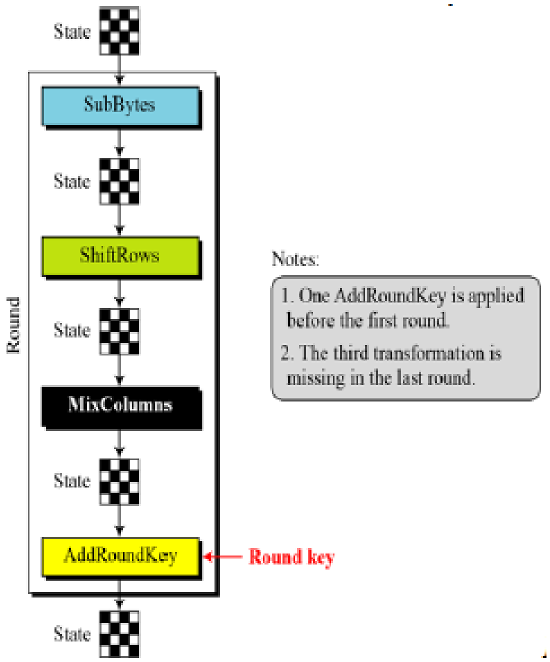
AES comprise 3 areas:

1. Security

2. Cost

3. Implementation.

It's possible that the Advanced Encryption Standard (AES) is a non-Feistel cipher that encodes and decrypts 128-bit knowledge blocks. The number of rounds might range from 10 to 14. The quantity of rounds determines the key size, which can be 128 bits, 192 bits, or 256 bits respectively.


State
SubBytes
State
ShiftRows
State
MixColumns
State
AddRoundKey
Round key
State
Round
Notes:
1. One AddRoundKey is applied before the first round.
2. The third transformation is missing in the last round.

AES employs four distinct kinds of transformations in order to ensure its users' safety: replacement, permutation, mixing, and the addition of keys.

Substitution

A non-linear stage of the substitution process in which every single memory module of the computer is replaced with another according to a table of specified operations.

Permutation

A phase in the transposition process that requires moving cyclically through a clear variety of steps for each and each row of the state.

Mixing

A intermixture operation that operates on the columns of the state, combining the four bytes in every column.

Key-Adding

During the AddRoundKey phase, the subkey and the state are merged into a single value. Every subkey is the same size as the state it belongs to since it is produced from the most important key using Rijndael's key schedule. This process is repeated for every sphere. The subkey is created by using bitwise XOR to combine each computer memory segment of the current state alongside the corresponding computer memory unit of the subkey. This process creates the additional subkey.

5.1 AES encoding & cryptography algorithmic rule

The Advanced Encryption Standard, also known as AES, is a mathematical guideline for playing encoding (and the reverse, decryption), which may be a sequence of well-defined stages that may be followed as a procedure. This guideline was developed by the National Institute of Standards and Technology (NIST). The information in its unencrypted form is commonly referred to as plaintext, whereas the information in its encrypted form is referred to as cipher text. The plaintext message contains all of the same information that is contained in the cipher text message; however, the cipher text message is not in a format that can be decoded by a person's or computer's without the right mechanism to decipher it; instead, it is designed to look like random gibberish to individuals who are not supposed to scan it. The data encryption method is dynamically altered in response to the key, which in turn modifies the algorithm's methodical functioning. The message cannot be encoded or decoded using the encryption since we do not have the key.

5.1.1 AES Encryption Algorithm

```
Cipher (byte in [4*Nb], byte out [4*Nb], word w [Nb*(Nr+1)]) begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr–1
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state,w[round*Nb,(round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
```

```
out = state
end
```

5.1.2 AES Decryption Algorithm

```
InvCipher(bytein[4*Nb],byteout[4*Nb],word w[Nb*(Nr+1)])
Begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    for round = Nr-1 step -1 downto 1
        InvShiftRows(state)
        InvSubBytes(state)
        AddRoundKey(state,w[round*Nb, (round+1)*Nb-1])
        InvMixColumns(state)
    end for
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[0, Nb-1])
    out = state
```

6. CONCLUSION

Cloud computing has the potential to be an exciting and developing technology for the next generation of information technology applications. Knowledge security and privacy concerns are the obstacles that must first be overcome before cloud computing can become widespread. When it comes to making decisions, one of the most important things an organization can do is analyze the information and data they have. However, minimizing the cost of storing and processing information is a requirement that must be met by all businesses. Because of this, no business will be able to upload their data or expertise to the cloud unless there is trust established between the cloud service providers and their customers. Researchers have come up with a number of different strategies in order to secure knowledge and achieve the best level of information security possible within the cloud. However, there are still a few holes that need to be filled by simplifying these methods. There is still a lot of work to be done within the realm of cloud computing in order to make it acceptable to customers of cloud services. In this study, a survey of several strategies concerning data security and privacy, with a specific focus on the storing and using of data within the cloud, was carried out with the purpose of providing information protection within cloud computing environments in order to construct trust between cloud service providers and their clients.

7. REFERENCES

[1] Carlin, Sean, and Kevin Curran. "Cloud computing security." (2011).

[2] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.

[3]https://cloudacademy.com/cloud-computing/what-is-cloud- computing-introductory-course/

[4].https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[5].Huiming Yu, Nakia Powell, Dexter Stembridge and Xiaohong Yuan, ―Cloud Computing and Security Challenges‖, 2012 ACM Publication.

[6].Hassan Mathkourand, B. Al-Sadoon and Ameur Touir, ―A New Image Steganography Technique‖, *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2008.

[7]Qingzhong Liu, Andrew H. Sung, Zhongxue Chen and Xudong Huang, ―A JPEG-Based Statistically Invisible .

[8].A. E. Mustafa, A. M. F. ElGamal, M. E. ElAlmi and B. D. Ahmed, ―A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit‖, *Research Journal Specific Education Faculty of Specific Education Mansoura University*, pp. 752-767, 2011.