Cryptography in Cloud Computing

1st Meet Gor

KJ Somaiya College of Engineering
Department of Information Technology
gor.m@somaiya.edu

2nd Pushpak Gupta

KJ Somaiya College of Engineering
Department of Information Technology
pushpak.gupta@somaiya.edu

3rd Ishaan Gurnani

KJ Somaiya College of Engineering
Department of Information Technology
ishaan.g@somaiya.edu

4th Paarth Kapur

KJ Somaiya College of Engineering
Department of Information Technology
paarth.kapur@somaiya.edu

5th Alekhya Gorugantu

KJ Somaiya College of Engineering
Department of Information Technology
alekhya.g@somaiya.edu

Abstract –

Cloud computing refers to the supply of computing services via the internet as opposed to storing files on a proprietary hard drive or local memory device. Servers, storage, databases, networking, and software are examples of computing services. The main reason and major benefit of using the cloud is that the user can save and access the stored data in the cloud from anywhere at any time, as well as receive all of its services for a reasonable cost.

Cloud computing is currently a developing and rapidly rising technology that is widely used all over the world. It makes advantage of the power of Internet-based computing, and data, information, and other resources are sent to the user on-demand through computer or device. Various industries that include health care, banking and education are drifting towards this technology, all because of the efficiency provided by the system which is powered by pay as you use model and hence it takes care of the bandwidth, data movement, transactions and storage information.

Security has always been a big concern with cloud computing because the information stored in the cloud is not directly maintained by the customer. To overcome the security issues various cryptography algorithms are proposed. This paper focuses on the basics of cloud computing and discusses various cryptography algorithms present in the existing work.

I. INTRODUCTION

The cloud is a frequent term for an Internet-accessible organization that is concealed from users. Cloud computing can be defined as a technology combination that delivers hosting and storage services through the internet. Cloud computing can be classified as public, private, or hybrid.

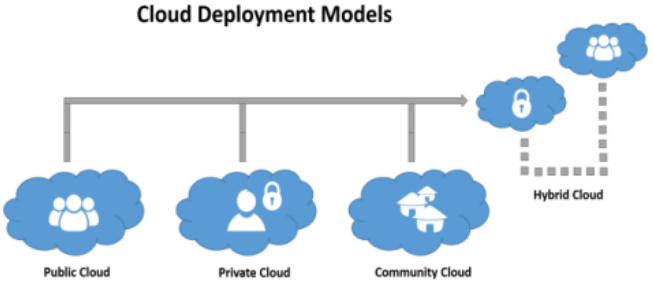
The most significant advantage of cloud computing is its low cost, increased storage capacity, and flexibility.

Yet, the primary issue in cloud computing is security and privacy, and this is emerging as a significant challenge that influences cloud computing fulfillment. Cloud safety includes the practices and software that are needed to keep cloud computing services safe from cyber threats. Cryptography is used frequently to ensure that information is safe, private, and correct in cloud computing. But the answers we have now aren't good enough nor do they work very well.

A. Cloud Computing:

Cloud computing is usually described in one of two ways. Either based on the deployment model, or on the service that the cloud is offering.
Based on a deployment model, we can classify cloud as:

- Public
- Private
- Hybrid
- Community cloud



Depending on the user or business need the different types of the cloud are available. There are four types of clouds available.

1. *Private Cloud:* A private cloud can be accessed by a single group or a single organization It is managed by a third party or organization. The private cloud is highly secure and flexible so the private cloud is often used by larger organizations or the government sectors.

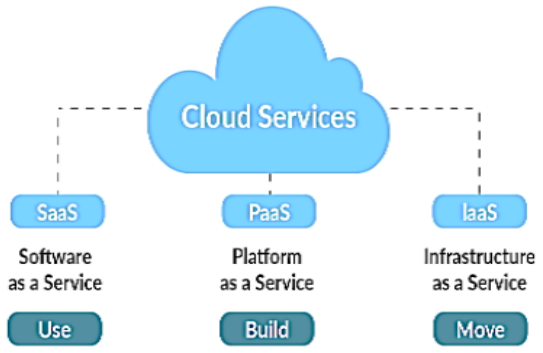
2. *Public Cloud:* A public cloud can be accessed by any user with an internet connection and want to pay as per their usage The files are hosted by a third party.
   Example Amazon, Windows Azure Service Platform and salesforce.

3. *Community Cloud:* A community cloud will be accessed by two or more organizations that have similar cloud requirements.

4. *Hybrid Cloud:* A hybrid is the combination of two or more cloud (public, private , and community)

   Based on a service the cloud model is offering, we are speaking of either:

   • IaaS (Infrastructure-as-a-Service)
   • PaaS (Platform-as-a-Service)
   • SaaS (Software-as-a-Service)
   • or, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service



Depending on the want of the buyer on the thanks to use the gap and sources associated with the cloud, the cloud provider issuer will provide the buyer greater or much less manipulation over their cloud. For instance: if it'll be for commercial enterprise use or non-public domestic use, the cloud want is also of assorted types.

There are 3 forms of cloud that provide software program as a Service (SaaS), Infrastructure as a provider (IaaS), platform as a provider (PaaS).

1. *Software as a provider:* SaaS, additionally called cloud software services. SaaS is controlled with the help of employing a third-party. Saas is used maximum generally utilized in commercial enterprise because of the very fact it does now now not require the founding of the software at once withinside the patron machine, the software is immediately run through the net browser.

Some common examples of Saas are GoToMeeting, Google Apps

2. *Infrastructure as a provider:* IaaS presents many laptop sources, hardware, software program, and garage tool on consumer demand. IaaS customers can get the correct entry to the provider through the utilization of the net. Some common examples of IaaS are Amazon, three Tera, GoGrid.

3. *Platform as a service:* A PaaS machine goes grade better than the code as a Service setup. A PaaS provider gives subscriber's get right of entry to the weather that they require to extend and perform programs over the software. Several instances for PaaS is J2EE, Ruby, and LAMP.

II. Related Work

Data security in cloud has been a main point of researcher, but talking about the all issue of data security will not solve the problem, that way most of the researcher focus on a particular point or weaknesses of data security in cloud.

Some are focusing on creating a better encryption to ensure that the share network are secure when we send a file, but their finding are not the same; some use asymmetric algorithm, some combine both asymmetric and symmetric algorithm to come with a better encryption.

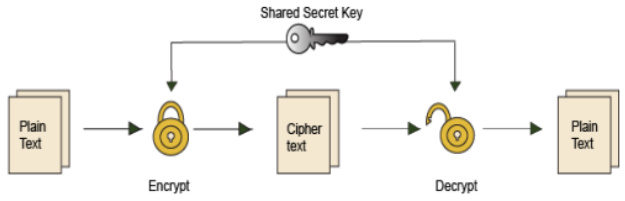
Other researchers focus on creating a third party audit to analyze if the cloud provider has a good security, to ensure their client that their data are well secure, other focus on creating a scheme and the rest are focusing in particular topic such as remote data integrity.

We can see that most of the researcher focus on creating a new encryption or using a third party to investigate on behavior of the client and other focus on

creating a scheme to make sure that the cloud has a good design and security at the high level, but no one has focus on how a new company or client will choose a particular encryption for it file before moving to cloud because all the data doesn't have the some value so a different encryption will be needed for each data, after choosing you can determine which cloud provider has that encryption and by doing that you will save the cost because you can use a combination of private cloud and public cloud depending of your data value.

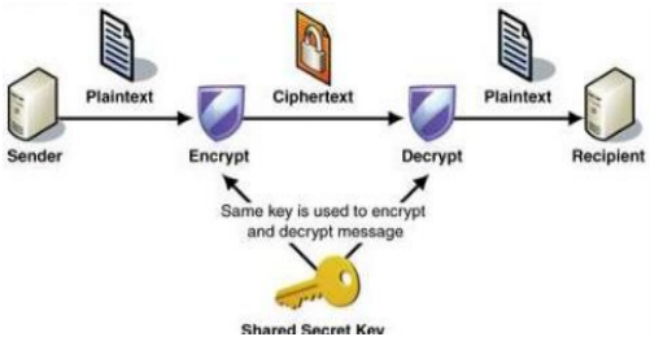
III. METHODOLOGY

Cryptography is the process of protecting information from unwanted parties by converting it into an unreadable form. The most essential reason for cryptography is to protect information from third parties. In order to achieve security in three areas: confidentiality, integrity, and availability. Cryptography is primarily concerned with the security of information within the cloud. There are three types of algorithms: (i) symmetric key based algorithms, (ii) asymmetric key based algorithms, also known as public-key collection of rules and (iii) Hashing



A. *Symmetric Key based algorithm*

These algorithms are classified into two types: Stream and block cyphers The input is taken as a fixed-size block of plaintext in block cypher as a result of the type of asymmetric encryption algorithm, the fixed-size key is applied on the plain text block, and then the same size the output block as plaintext is acquired. In the case of Stream Cipher, one bit is encoded at a time.

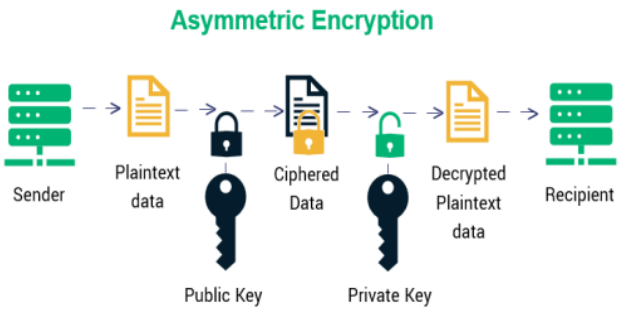


1) Data Encryption Standard: DES is the prototypical block cipher-an algorithm that takes a fixed-duration string of plaintext bits and transforms it into another ciphertext bitstring of the same period via a number of complicated operations. The block length for DES is 64 bits. DES also employs a key to customize the transformation, so that decryption is allegedly only possible by means of those who understand the actual key used to encrypt.

2) Diffie Hellman: A set of rules intended to generate a shared secret key for securely exchanging data. DH is one of the earliest, practical instances of public key exchange in the field of cryptography, and it serves as the foundation for a slew of authenticated protocols.

B. *Asymmetric Key based algorithm*

Asymmetric - two distinct keys are used. Anyone on the network has access to the public key. The public key is used to encrypt data. Only the private key has the ability to decode that info. The private key is kept secret and is required to keep information secure. The advantages of using asymmetric key encryption are that it provides greater scalability and key distribution than symmetric systems.



1) RSA: it is one of the first and earliest asymmetric cryptosystems. It is still the most widely used and utilized cryptosystem. It includes two keys: a secret key and a public key. Messages scrambled with the public key can be deciphered using the private key. In this verification process, the server authenticates the public key by inscribing a unique message with its private key, which is known as digital signature. The client's thumbprint is then returned. It then validates using the server's public key.

2) ElGamel: Elgamal is an asymmetric algorithm used for key exchange and for sharing digital signatures. Discrete logarithms' utility is the foundation of El Gamal. It is founded on these numbers' logarithmic properties or estimates. Diffie-Hellman has been updated and extended in ElGamal.

C. Hashing Key Cryptography

With the exception of message digests, hash functions are referred to as one-way encryption. Hash values are computed based on the plaintext rather than a set length to make it impossible for the plaintext's details or length to be recovered. Many operating systems commonly use the hash function to encrypt passwords. It also provides a way to verify programme integrity checking. It serves to protect a file from being altered by a malware or hacker. Hash methods are commonly used to provide a digital fingerprint of a file's contents.

1) MD5: The commonly used MD5 hash function converts messages of variable length into outputs of a fixed length of 128 bits using a hash value of 128 bits. The information message is first divided into 512-bit chunks and then cushioned so that its entire length can be distinguished by 512 bits. The sender uses the public key to encrypt data, and the recipient uses the private key to decode it. In terms of security and performance, MD5 is superior. Since its introduction in 1992, the MD5 hash algorithm has gained enormous popularity. It has been used for many different purposes; for instance, it is available as a native tool in almost all Linux and Unix versions.

2) SHA-1: A 160-bit (20-byte) hash value is produced by the cryptographic hash algorithm known as SHA-1, or Secure Hash Algorithm 1. Although the functions' structure is comparable to that of MD5, several changes and modifications have been made in order to improve their security.

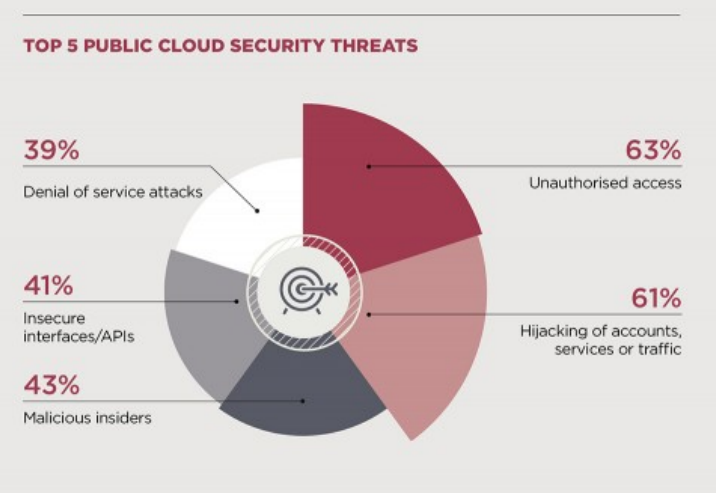
IV. SECURITY IN CLOUD

Gartner, an American information technology research and advisory firm, recently suggested that cloud computing, as used for service-enabled applications, should be considered.

Applications had another seven years before reaching market maturity. Scalability, interoperability, shared environment, and security are some of the issues it is currently dealing with, in addition to other business-related issues. There is no denying that cloud resources are virtualized; different cloud service users share the same infrastructure and platform for application development and data storage.
One key area of interest is architecture set, asset alienation, and data segregation. Any unauthorized and ferocious access to a cloud service user's sensitive data may jeopardize its completeness, secrecy, and privacy.

A. Cloud Threats

Several of the threats were analyzed over a period of time, and it was found that a large amount of data was compromised by Thefts and Unauthorized Access. Other small percentage of security threat was due to Loss, Combination, IT incident, Improper Disposal etc.



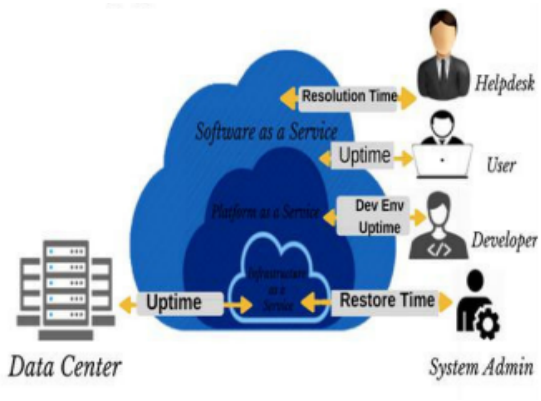
B. Technical Issues

- *Security*

Security can be defined as “how information can be locked safely”. The fact that the priceless enterprise information will dwell outside the firm firewall raises grave concerns.
Many high sensitive data can be exposed publicly if necessary measures are not taken. Hacking and different attacks to cloud structure would impact multiple clients even if merely one site is broken into. These risks can be impaired by using safety applications, encrypted data file schemes, data loss software, and purchasing security hardware to track out-of-the-way conduct across servers.

- *Distributed Responsibilties*

The main security issue is that the user must check before uploading the delicate data into the cloud storage. They must also take decent security measures such as using 32-bit encryption. This is a vital part because data can be secured if it is encrypted before saving it in the cloud store. Thus, even if intrusion happens, there is a very minimum chance of the data getting stolen. Encryption in the cloud is given in the diagram below.



- *Fault Tolerance and Failure Recovery*

The data centers are merely responsible to process tremendous amounts of data each day. Cloud services can face the problem of loss of data due to the failure of the system of the cloud. The shortage of power supply, low space or breakdown of the main system could lead to failure.

C. Challenges Faced in Cloud Computing

These are some of the challenges that are needed for security and their knowledge is necessary for mitigation purposes.

- *Privileged User Access*

Any client that accesses data outside the enterprise then the user has to take permission or buy membership for prevention of data leak.

- *Data Location*

Any client that accesses data outside the enterprise then the user has to take permission or buy membership for prevention of data leak.

- *Availability*

These are some of the challenges that are needed for security and their knowledge is necessary for mitigation purposes.

- *Regulator Compliance*

The hosting providers should never allow external audits or allow installation of external new security certificates.

- *Recovery*

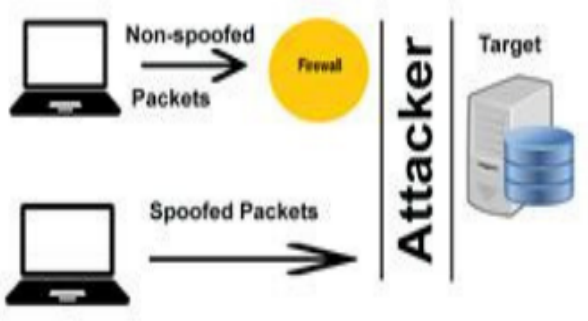
If under any condition the data is ruined by any disaster, man-made or natural, the providers should be able to deliver the backup data to the users on time.

D. Challenges Faced in Cloud Computing

Cloud Computing helps us to access data and information for particular organizations. Hackers and Attackers have found out loopholes to gain access to this information. Cloud Computing helps us to access data and information for particular organizations. Hackers and Attackers have found out loopholes to gain access to this information.

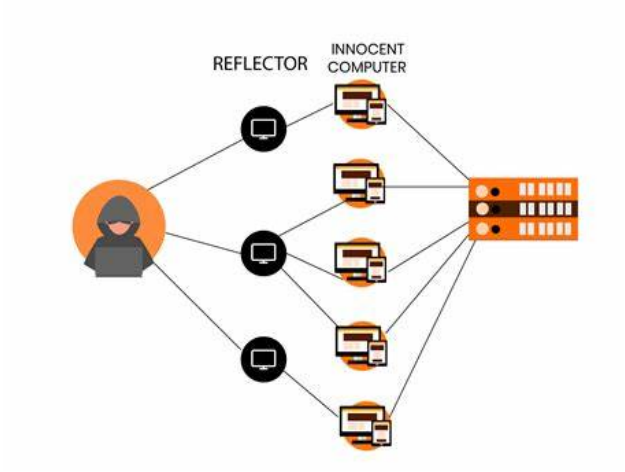
- *IP Spoofing*

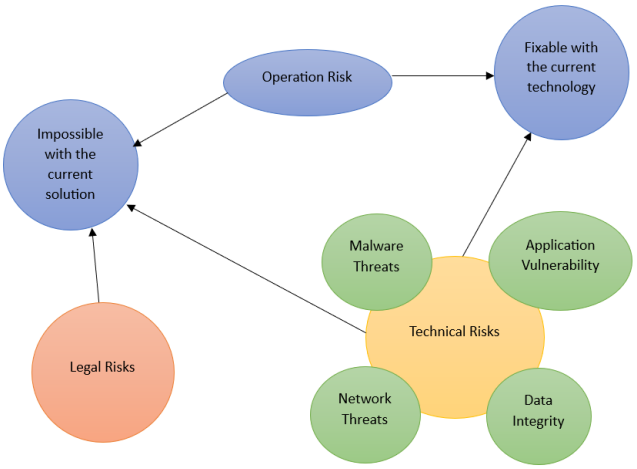
IP Spoofing is known as analysis of the data that is being sent over the network. When data is sent over the network the attacker manipulates the data. The manipulation is done in a way that the IP address of the trusted system and then modifies the packet information and then sends it to the receiving system.



- *DDOS Attack*

In this attack, DDOS the attacker spoofs the information and sends many requests of the data. The server gets confused and doesn't understand what to do with all these requests and finally ends up giving up authenticated data. The basic diagram of a DDOS attack is below:





- *Insecure Interface*

Interface is the model that helps the client to adhere to the cloud internal software. Management of data, identity management, monitor service and other functions that happen on the cloud are done through these interfaces. If the interface is not secure, then data theft is very easy.

- *Malicious Insider*

The insiders such as the employees or any user can manipulate the data, such that they can even sell the information to other organizations. This causes severe data leaks in cloud computing.

- *Data Loss or Leakage*

There are two processes taking place when data is being transmitted from host to client. First of all, data is being stored in a far place and secondly, data transmission happens from one mode of execution to modes that are multiple in nature. Thus, if any modification happen in between, the loss or leakage of data occurs

- *Malware Attack on VM*

Cloud Security can be compromised by the unwanted VM-based virus or tool-kits that are used to cloak the information sent to the server by the user. Same process can happen when the data is being sent from the server to the client. These viruses or malwares are also used to store the data such as registry information, system logs, and security program details. This flow charts shows us how these risks are interrelated:

V. CONCLUSION

The vital goal is to store firmly and access information in the cloud that is not controlled by the owner of the information. Software structures often have a couple of endpoints, typically more than one client, and one or more are given up servers. Those customer/server communications take place over networks that can not be depended on. communication takes place over open, public networks including the net, or nonpublic networks which may be compromised via external attackers or malicious insiders. Cryptography can defend communications that traverse untrusted networks. There are principal kinds of assaults that an adversary may try and perform on a community. Passive attacks contain an attacker listening on a community phase and attempting to examine touchy records as it travels. Passive attacks may be on-line (wherein an attacker reads traffic in actual-time) or offline (wherein an attacker without a doubt captures site visitors in real-time and perspectives it later—possibly after spending a while decrypting it). energetic assaults contain an attacker impersonating a purchaser or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them directly to their intended vacation spot (or dropping them absolutely).
This paper has given a clear view on cloud computing and its security issues using cryptography methods.

VI. REFERENCES

[1] Felix Bentil , Isaac Lartey, "Cloud Cryptography – A Security Aspect", May 2021 , DOI : 10.17577/IJERTV10IS050258

[2] P. S. Wooley, "Identifying Cloud Computing Security Risks", Contin. Educ., vol. 1277, no. February, 2011.

[3] Adee, R.; Mouratidis, H. "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography". Sensors 2022, 22, 1109. https://doi.org/10.3390/s22031109

[4] Rishav Chatterjee1, Sharmistha Roy, "Cryptography in Cloud Computing: A Basic Approach to EnsureSecurity in Cloud", July 2017

[5] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing", J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[6] Aws Jaber, Mohamad Fadli Zolkipli, "Use of cryptography in cloud computing", 2013 IEEE International Conference, DOI: 10.1109/ICCSCE.2013.6719955

[7] Ali Abdulridha Taha, Diaa Salama AbdElminaam and Khalid M Hosny, "NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment" International Journal of Advanced Computer Science and Applications(IJACSA), 8(11), 2017. http://dx.doi.org/10.14569/IJACSA.2017.081158

[8] "Cloud Computing – Cryptography", International Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Vol.8, Issue 7, page no. ppg231-g234, July-2021

[9] Simranpreet Kaur, Manvi Chauhan and Ankita, " Security in Cloud Computing using IDS", IJARSCT, 2021

[10] VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, "Single Cloud Security Enhancement using key Sharing Algorithm", Recent and Innovation Trends in Computing and 2016Communication, 2016.