International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Computing

Jocasta Lathisha L

21BCAS46, St Joseph's University

ABSTRACT

The distribution of various services, such as data storage, servers, databases, networking, and software, through the Internet is known as cloud computing. Pall storehouse has lost some of its appeal among people who require more storage capacity and among companies looking for a good data back-up solution. Lines can be saved to a remote database and recovered on demand thanks to a pall- grounded storage. Public and private services are both available; the difference between the two is that public services are provided online for a fee, whereas private services are provided on a network to individual users. The importance of information security is waning.

Introduction

The on-demand delivery of computer resources, such as servers, storage, applications, and services, through the internet is known as cloud computing. Users no longer need to own and maintain their own infrastructure in order to access and use computer resources as needed. This can range from storage of data and software applications to servers, databases, and networking services. Unlike traditional methods of storing data, cloud-based storage allows users to access their files from any location with an internet connection, eliminating the need for local storage devices. This technology offers numerous benefits, including cost savings, increased productivity, and security, making it a popular choice for individuals and businesses alike. Additionally, cloud computing provides increased speed and efficiency in accessing data and software, making it a highly efficient option for those seeking reliable and high-performance computing services.

Applications of Cloud Computing

Cloud computing is utilized by both companies and people in a wide range of fascinating and distinctive ways. For its Cloud Infrastructure Report 2021, the cloud management company CloudCheckr polled 304 IT and business stakeholders, and more than half of them stated that their infrastructure was already in the cloud.

Although many other organizations, both big and small, host the cloud, the most well-known ones are giant corporations like Amazon (Amazon Web Services), Microsoft (Azure), Apple (iCloud), and Google (Google Drive). Cloud businesses, often known as cloud service providers (CSPs), provide cloud-based services or applications. Customers may access and use the information they host from them in a flexible, controllable, and reliable manner thanks to the tools and data centers they host. Through any network connection, customers can effortlessly access their cloud-based data. Streaming video and music, backup storage for iPhones and other mobile devices, and cloud-based collaboration platforms like Microsoft One Drive and Dropbox are some of the most popular cloud computing apps that users might come across at work or in daily life. Along with a few of the instances described above, here is a quick look at a few other important application areas.

Understanding Cloud Computing

The term "cloud computing" refers to the penetration of information from the "pall," a virtual environment. Without having to be in a certain place to access it, service providers allow drug users to save data and operations on remote servers that can be accessed via the internet. Pall computing transfers the responsibility for data processing and scraping from the device to huge computer clusters in the internet. This makes it possible for drug users to access their information, work, and operations from any internet-connected device, wherever in the world. Pall computer services can be made available to the general public or a select group of drug users, with the latter only having access to private services. Additionally, a mongrel alternative that blends elements of both public and private pall services is available.

Advantages of Cloud Computing

Savings: Thanks to cloud computing, businesses no longer need to spend money on expensive hardware and software. Instead, they can use pay-as-you-go access to the necessary resources and services, which can eventually result in significant cost savings. You don't need to buy and maintain your own servers, which can be expensive and require trained personnel to operate. Instead, you can rely on cloud service providers who will take care of buying and managing equipment for you.

Strategic advantage: Due of the ease of access to the most recent programmes without the expense of costly installation, cloud computing might provide you an advantage over your rivals. This means you can quickly adopt new technologies and stay ahead of the curve.

High speed: Cloud computing enables faster deployment of resources, allowing you to get the resources you need in just a few clicks. This can be especially useful in situations where you need to scale up your infrastructure quickly.

Sustainability: By depending on shared infrastructure and effective data centres, cloud computing can be more ecologically friendly than conventional on-premises IT infrastructure for organizations. This allows them to use less energy and produce less carbon dioxide.

Automatic software integration: The cloud makes instant software integration possible and does not require further customization or integration work. This kind of time and resource saving can provide you more time to concentrate on your main business operations.

Reliability: Cloud hosting provides reliable and instant updates on changes, which can help you stay informed about your infrastructure and prevent any potential issues.

Mobility: Cloud services are easily accessible by employees in different locations with internet connectivity. This means your team can work from anywhere and collaborate more effectively.

Unlimited storage: The cloud provides a vast amount of storage space that can be increased at any point by paying a small monthly fee, ensuring that you can store a significant amount of data without any concerns about space constraints.

Collaboration: Cloud computing allows for secure and convenient collaboration among employees in different locations. You can easily share files and work on projects together, regardless of where you are.

Quick deployment: Cloud computing enables rapid deployment of the entire system, depending on the technologies used by the business. This means you can quickly set up and start using the cloud services you need, without having to wait for long installation times or complex configurations.

Disadvantages of Cloud Computing

Performance can vary: When employing cloud computing, our application’s performance can change when it’s running on a shared server that makes resources available to other companies. Because of the shared environment, any greedy activity or DDOS assault on one tenant could have an uncontrollable impact on the performance of your application. As a result, your application’s performance might not always be constant or predictable.

Technical problems: There will always be outages and other problems with cloud technologies. Even the best cloud service providers, although adhering to strict maintenance guidelines, occasionally run into these issues. These technical faults might cause delays and other problems by interrupting your business operations and producing downtime.

Risks related to security: The possibility of security breaches is one of cloud computing's key problems. Before utilizing cloud technology, it's crucial to realize that you would be giving a third-party access to every sensitive piece of information your business possesses. Due to this information sharing, hackers may be able to access your data, steal sensitive information, and jeopardize the security of your company.

Downtime: Another difficulty you could encounter while using cloud computing is downtime. Power outages, poor internet connectivity, service maintenance, and other problems could affect your cloud provider and briefly take the system offline. These interruptions can be annoying, and your company might not be able to function effectively during these times.

Internet Connectivity: Good internet connectivity is essential for accessing cloud services. Without a reliable internet connection, you won’t be able to access cloud services or retrieve data from the cloud. Any disruption in internet connectivity can lead to delays in business operations and cause other problems.

Bandwidth usage limitations: The bandwidth that customers can use is frequently constrained by cloud storage service providers. If your business uses more than the allotted amount, the extra fees could be very expensive, resulting in unanticipated costs that could harm your budget and bottom line.

Lack of Support: Cloud computing companies may not always provide proper support to their customers. They often expect users to depend on FAQs or online help, which can be a tedious job, especially for non-technical persons. The lack of adequate customer support can lead to frustration and delay in resolving issues, which could impact your business operations.

A study on Cloud Computing security algorithms

1. RSA Algorithm
2. Blowfish Algorithm
3. Diffie Hellman Key Exchange (D-H)
4. Elliptic Curve Cryptography Algorithm
5. Data Encryption Standard (DES) Algorithm
6. El Gamal Encryption
7. Advanced Encryption Standard (AES)
8. Digital Signature Algorithm (DSA)
9. Triple Data Encryption Standard (3DES)
10. MD5 (Message-Digest Algorithm 5)

(1) RSA Algorithm

The idea behind it, which was first presented in 1977 by Ron Rivets, Adi Shamir, and Len Adelman, includes encrypting the data and then storing the encrypted data on the cloud. Users seek access to the data from the cloud service provider and are given permission to do so when they need it. A third party can ask for proof for a certain amount of message blocks that are translated into integer values in order to spot fraudulent behavior from cloud service providers. Both a Public Key and a Private Key are employed by RSA, the former of which is known solely to the data owner and the latter of which is shared by all cloud users. The cloud service provider performs the encryption, while the cloud user or client does the decryption.

2. Blowfish Algorithm

Bruce Schneier created the symmetric key Blowfish algorithm, which is a well-liked encryption technique. Although it requires a huge key length that may range from 32 to 448 bits, it is identical to the DES algorithms in that regard. The 16-round technique guarantees that even if the message's measures not a multiple of eight bits, it is still encoded. It can encrypt data of different sizes.

The algorithm splits the raw text into two portions, each 32 bits long. In order to construct the value that will be transmitted via the transformation function F, the left part of the message is XORed with components of the P-array. Overall, the Blowfish algorithm is a strong encryption algorithm that can effectively protect sensitive data. Its large key size and variable message size make it a versatile option for encryption, while its multiple rounds of encryption enhance its security.

3. Diffie Hellman Key Exchange (D-H)

Whitfield Diffie and Martin Hellman's groundbreaking development in the area of cryptography is the Diffie Hellman key exchange algorithm. It is regarded as the first real-world use of public-key cryptography and offers a safe way to exchange cryptographic keys over a public network. This algorithm enables two users to exchange a secret key across an untrusted network without needing to be aware of each other's secrets beforehand. This is made possible by using challenging calculations involving discrete logarithms of enormous prime numbers. A prime number (P) and a second number (G), which acts as the primitive root of P, are both necessary for the application of this procedure. The complexity of determining the discrete logarithms of these huge prime numbers contributes to the Diffie Hellman algorithm's security by making it nearly impossible for a third party to intercept and decode the exchanged key. Users can safely converse and transfer sensitive information over public networks using this method without worrying about being intercepted or eavesdropped by nefarious third parties.

4. Elliptic Curve Cryptography Algorithm

In 1985, Neil Koblitz from the University of Washington and Victor Miller from IBM made the discovery of the Elliptic Curve Cryptography Algorithm, or ECC. ECC is a kind of public key encryption that uses discrete algorithms to produce concise and effective cryptographic keys. ECC is a cutting-edge method of encryption because it makes use of the algebraic structure of elliptic curves over finite fields with small key sizes. The ECC functions by using two locations (x, y) that satisfy the equation y2 = x3 + axe + b under a specific condition (4a3 + 27b2 = 0) and sharing a secret key. Public keys are represented by points on the curve, while private keys are encrypted using random integers. Some integer factorization techniques that are used in cryptography also make use of ECC. Overall, ECC is a very strong encryption method that uses smaller, quicker cryptographic keys to provide increased security. Strong and effective keys can be produced using elliptic curves and discrete algorithms in ECC, which enables their usage in a variety of cryptographic applications.

5. Data Encryption Standard (DES) Algorithm

The National Institute of Standards and Technology (NIST) created the Data Encryption Standard (DES) in January 1977 as a cryptographic method. DES is a symmetric-key block cypher, which means that both encryption and decryption rely on the same secret key. A 64-bit plaintext is converted into a 64-bit ciphertext when using DES to encrypt data. Similarly, when decrypting the ciphertext, the process reverses to yield the original plaintext. The encryption and decryption processes use a 56-bit cipher key, which is used to generate different 48-bit round keys for each of the sixteen rounds of the algorithm. The initial and final permutations, as well as sixteen rounds of a Feistel cypher, make up the DES encryption process. The initial permutation reorders the bits of the plaintext, while the final permutation reorders the bits of the ciphertext. The Feistel cipher is a cryptographic technique that divides the plaintext into two halves, which are then manipulated using a function that depends on the current round key.

6. El Gamal Encryption

Asymmetric key encryption is performed using the El Gamal encryption system in public-key cryptography. It is based on the Diffie-Hellman key exchange procedure, which employs cryptography, and was created by Taher Elgamal in 1984. Software like PGP and the GNU Privacy Guard also support ElGamal encryption. It must not be mistaken with the ElGamal signature scheme's variation, the Digital Signature Algorithm. ElGamal encryption can be used with any cyclic group G and its security depends on how challenging it is to solve a particular discrete logarithm calculation issue in that group.

7. Advanced Encryption Standard (AES)

NIST has recommended Advanced Encryption Standard (AES) as an alternative to DES for encryption. AES is made up of the cypher blocks AES-128, AES-192, and AES-256. Communications are encrypted and decrypted in 128-bit blocks, with each block using a different key length of 128, 192, or 256 bits. Symmetric cyphers, also called secret key cyphers, use the same secret key for both encryption and decryption, therefore both the sender and the recipient must have access to it. 192- or 256-bit key lengths are required for really confidential information. Depending on the key length used, different numbers of rounds are necessary for encryption; for 128-bit keys, there are 10 rounds; for 192-bit keys, there are 12 rounds. There are 14 rounds for 256-bit keys as well.

8. Digital Signature Algorithm (DSA)

The digital signature algorithm (DSA), developed by the National Institute of Standards and Technology (NIST), became the accepted method for creating digital signatures in 1991. Along with RSA, it is currently one of the most widely used algorithms for digital signatures. DSA does not require the usage of private keys to encrypt or public keys to decrypt message digests, in contrast to encryption and decryption. The DSA authenticates the signature using the public key, although the process is more difficult than it is with RSA.

9 Triple Data Encryption Standard (3DES)

A modified version of the Data Encryption Standard (DES) algorithm is called Triple-DES (3DES), which uses three 64-bit keys instead of one. By using three keys, the key length is increased to 192 bits, which eliminates many of the attacks that can be used to break DES quickly. Additionally, using 3DES is straightforward as it is easy to modify existing software. When using Stealth, the user inputs the complete 192-bit key (24 characters), which is then divided into three 64-bit subkeys by the Triple-DES Dynamic Link Library (DLL). The subkeys are padded if needed, and encryption is performed using the same procedure as regular DES, repeated three times. It is named Triple DES because of this procedure. Overall, 3DES is a more secure encryption method than standard DES because to its benefit of shown dependability and a greater key length. the same as with conventional DES, the encryption process is done three times for further protection.

10. MD5 (Message-Digest Algorithm 5)

The fifth-generation Message-Digest Algorithm, or MD5, Despite being shown to have flaws, MD5 is still commonly used in many different applications, such as file integrity checking and security protocols like SSH, SSL, and IPsec. The main goal of MD5 is to confirm that a file hasn't been changed or tampered with in any manner since it was created. This is done by utilizing the MD5 technique to create a hash value for the file, then comparing it to a hash value created for the same file at a later time. The file is regarded as intact and unaltered if the hash values match. Digital signatures, password storage, and encrypted communication are some additional security features and applications offered by MD5, in addition to file integrity verification. However, as a result of the MD5 flaws found, some applications increase its security by taking additional measures such employing several hash algorithms or adding a salt value to the plaintext. Before using the MD5 hashing algorithm, the plaintext is supplemented with a random string of characters to add a salt value. Due to the necessity to separately calculate each salt value, it becomes more challenging for attackers to crack the hash using precomputed tables of hash values.

Triple Data Encryption Standard (3DES)

A popular cryptographic scheme for protecting data both in transit and at rest is called Triple Data Encryption Standard (3DES). It operates on data in fixed-sized blocks of 64 bits and is a symmetric-key block cypher, which means it utilizes the same key for both encryption and decryption. Each block of data is encrypted using the Data Encryption Standard (DES) cypher three times with a 56-bit key in 3DES. This method, called "triple encryption," offers more security than DES, which is weak against brute-force attacks because of its comparably low-key length. 3DES can be used in cloud computing to encrypt data that is stored or sent over the internet.

For example, a cloud service provider might use 3DES to encrypt data that is stored in their data centres, to protect it from unauthorized access. Similarly, 3DES can be used to encrypt data that is transmitted between the cloud provider and their customers, to prevent eavesdropping and other forms of interception.

Even though 3DES has been in use for a long time and is still regarded as a reliable encryption method, it is now viewed as an outdated encryption standard. This is because newer, safer algorithms like the Advanced Encryption Standard (AES), which provides better security and faster performance, have generally replaced it. As a result, even though 3DES can still offer a respectable level of security, it might not be enough to defend against some of the more advanced attacks that are now feasible. In order to provide a thorough defense against contemporary threats, it is advised to employ 3DES in conjunction with additional security measures like network firewalls, intrusion detection systems, and multi-factor authentication.

DISADVANTAGES: -

1. Slower performance: Triple DES requires more processing time and resources than other modern encryption algorithms, such as Advanced Encryption Standard (AES), because it applies the DES cipher three times. This can impact performance in high-volume or time-sensitive applications, such as real-time communication or financial transactions**.**

2. Key management complexity: Triple DES requires careful management of its two or three keys, depending on the mode used. This can be more difficult to manage than the single key used in some other encryption algorithms, such as AES. In addition, if a key is compromised, it may be necessary to replace all three keys, which can be a time-consuming process.

3. Vulnerability to some attacks: Although 3DES is still considered secure, it is vulnerable to certain types of attacks. For example, the key scheduling algorithm used in 3DES is not as strong as in some other encryption algorithms, which can make it vulnerable to certain types of attacks. In addition, 3DES has a fixed block size of 64 bits, which can make it susceptible to certain types of attacks, such as birthday attacks.

4. Limited key length: Triple DES uses a key length of only 56 bits, which is considered too short to be fully secure against modern attacks. While the algorithm applies the key three times, it still results in an effective key length of only 112 bits, which is less than the 128-bit key length used in AES. This makes it vulnerable to brute-force attacks that can be used to guess the key.

5. Deprecated: Triple DES is an older encryption algorithm that is no longer recommended for use in new systems. Instead, newer encryption algorithms such as AES and ChaCha20 are preferred due to their better performance and stronger security properties. This means that using 3DES may not be future-proof, and could result in the need to upgrade to a newer encryption algorithm at a later date.

Ways to overcome these disadvantages: -

1. Performance: More effective encryption algorithms like Advanced Encryption Standard can be used to overcome 3DES's poor performance. (AES). Compared to 3DES, AES is quicker and offers greater security.

2. Key maintenance: Systems that automate the distribution and maintenance of encryption keys can be used to reduce the complexity of key management. These mechanisms make sure that the keys are safe and that only authorized individuals can access them.

3. Key Length: Triple Data Encryption Algorithm, a more secure variation of 3DES, can be used to extend 3DES's key length. (TDEA). TDEA is more secure than 3DES since it employs a key length of 192 bits.

4. Assaults: Stronger encryption methods like AES can be used to reduce the vulnerability to assaults. AES has been created to be resistant to a variety of attacks, such as meet-in-the-middle and brute force assaults.

5. Compatibility: To get over compatibility problems, one might use current encryption protocols and techniques that work with current systems. For instance, modern encryption algorithms like AES are supported by the Transport Layer Security (TLS) protocol, which is widely used to secure communication over the internet.

Overall, one should combine effective encryption algorithms, key management systems, and contemporary encryption protocols that offer higher security, faster performance, and better compatibility to overcome the drawbacks of 3DES.

MD5 (Message-Digest Algorithm 5)

Ronald Rivest created the MD5 (Message-Digest Algorithm) in 1991. It was initially intended as a cryptographic tool to check the accuracy of data, validate digital signatures, and guard against data manipulation.

MD5 works by taking a message of any length as input and applying a series of mathematical operations to produce a fixed-length output. The output, known as the message digest, is a unique representation of the original message and is typically represented as a hexadecimal number. Many different applications, such as password storage, digital signatures, and data integrity checking, use MD5. However, due to security flaws discovered, MD5 is no longer regarded as a secure hash algorithm for delicate applications. It is especially susceptible to collisions, which occur when two distinct messages generate the same hash value and can be used by attackers to counterfeit digital signatures or get around authentication systems. MD5 can be used to verify the integrity of data stored in the cloud. For example, if you upload a file to a cloud storage service, you can calculate the MD5 hash of the file before uploading it and then verify the hash after downloading it from the cloud to ensure that the file was not tampered with during the transfer.

DISADVANTAGES: -

MD5 (Message-Digest Algorithm 5) has several disadvantages, which include:

1. Weaknesses: MD5 is susceptible to collision and preimage assaults, among other types of attacks. Attackers may discover two distinct inputs that produce the same hash value during collision attacks, which might result in security lapses. Preimage attacks allow attackers to locate an input that produces a certain hash value that can be exploited to create fake digital signatures or get around authentication protocols.

2. Security flaws: MD5 has been discovered to be less secure than more recent hash algorithms like SHA-256 or SHA-3. For critical applications, more secure hashing algorithms are advised.

3. Slow processing: MD5 is relatively slow compared to newer hash functions, which can be a performance issue in some applications.

4. Limited hash length: MD5 generates a fixed-length hash value of 128 bits, which might not be enough for many applications. Longer hash values produced by more recent hash methods like SHA-256 or SHA-3 offer higher security.

5. Lack of key strengthening: MD5 does not provide key strengthening, which can make it vulnerable to brute-force attacks.

Ways to overcome these disadvantages: -

1. Use more secure hashing algorithms as opposed to MD5: SHA-256 or SHA-3 are more secure hashing algorithms that should be used in place of MD5. These algorithms are less prone to assaults and offer greater security characteristics.

2. Implement safe key management. Public key cryptography and digital signatures are two key management techniques that should be used to enable secure communication in cloud computing environments. This can stave off assaults like man-in-the-middle attacks and data tampering.

3. Use hardware acceleration: Hardware acceleration can be utilized to increase the speed of hashing methods. Numerous cloud service providers provide hardware acceleration services, which can greatly enhance the speed of cryptographic processes.

4. Maintain software up to date: To make sure that any known vulnerabilities are patched, it’s crucial to maintain software and libraries up to date. This can aid in preventing attacks that take advantage of the hashing algorithm’s known vulnerabilities.

5. Conduct routine security audits: Routine security audits can assist in identifying weaknesses in the cloud computing environment and guarantee that security measures are current and efficient. By doing this, attacks that take advantage of holes in the hashing algorithm or other security measures can be avoided.

Conclusion:

In conclusion, because to their known flaws, neither MD5 nor 3DES are advised for use in contemporary cloud computing systems. While 3DES has a relatively small key length and there are more secure encryption algorithms like AES available, MD5 is susceptible to collision attacks. To protect the security of data, it is advised to utilize more secure hashing algorithms like SHA-256 for hashing and AES for encryption in cloud computing environments.