Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Cryptography Techniques in Cloud Computing and their Role and Applications

[1]Rakhi Tiwari, [2] Dr. Ajay Jain
[1]Student, [2]Professor
Department of Computer Science
Dr. A.P.J. Abdul Kalam University, Indore, India

Article Info
Page Number: 2021-2029
Publication Issue:
Vol. 71 No. 3 (2022)

Abstract
Introduction: Stream cyphers and block cyphers, as well as hash functions, are the most common types of cyphers used in cryptography. In order to safeguard and preserve the integrity and confidentiality of a piece of information, a method known as encryption is used. There are primarily two types of encryption algorithms: public-key and private-key. Two types of public key encryption exist: (1) algorithms that use just a single key, such Diffie-Hellman and RSA; and (2) methods that use both a single key and several public keys. Among the primary differences between the two is the usage of keys in each.
Aim of the study: the main aim of the study is to Cryptography Techniques In Cloud Computing And Their Role And Applications
Material and method: The use of cloud cryptography protects sensitive data even when it is stored outside of the corporate IT environment. To safeguard data in the cloud, we must rely on a variety of cryptographic approaches and algorithms since we lack a mechanism that allows us to exert physical or logical control over the storage of data in this manner.
Conclusion: Users may access cloud computing resources and services over the internet, provided by cloud service providers, at any time and from any location. The fact that every enterprise is moving its data to the cloud implies they are relying on the storage services offered by the cloud provider. As a result, several assaults on that data must be guarded against.
Keywords: Cloud Computing, Cryptography, Encryption, Virtualization, Algorithm etc.

Article History
Article Received:*15 April 2022*
Accepted: *28 May 2022*
Publication: *20 July 2022*

1. Introduction

1.1 Overview

Cloud computing is a kind of computing that makes use of the Internet to provide computer services. Individuals and businesses may make use of cloud services to access software and hardware that is managed by third parties located in different places across the world. Cloud-based services include things like online file storage, social networking sites, e-mail, and corporate applications, to name a few examples. Because of the cloud computing design, information and computer resources may be accessible from almost any place through a network connection. Every one of these resources is made accessible to all users and businesses alike via the utilisation of a common pool of resources referred to as "the cloud." To put it another way, cloud computing is a methodology for providing on-demand network access to a shared pool of customizable computing resources (such as network bandwidth and server capacity) that can be promptly supplied and released with the least amount of

administration effort and service provider interaction. Every organisation is shifting to the cloud in order to take advantage of these benefits. It is vital to protect sensitive data in order to prevent unauthorised access, modification, or denial of service. "Cloud security" refers to the process of "securing operations, calculations, and data storage" in the cloud (databases hosted by the Cloud provider). The three fundamental goals of data security are availability, integrity, and authentication, in that order. Integrity and Confidentiality are essential. Cloud data is protected against unwanted access via the use of cryptography. Modern cryptography is comprised of a combination of three main types of algorithm. Asymmetric-key algorithms, symmetric-key algorithms, and hashing are examples of these algorithms. Data integrity is protected by using hashing algorithms, which are mathematical formulas.

The basic aim of data cryptography is to scramble information in such a way that it becomes incoherent or useless during the transmission or storage of data. In this context, it is referred to as Encryption. The basic purpose of cryptography is to prevent data from being accessed by unauthorised parties. Decryption, on the other hand, is the process of recovering the original data after it has been hidden by encryption. When it comes to cloud storage encryption, both symmetric-key and asymmetric-key approaches are available. When utilised with large databases, such as those available in cloud storage, asymmetric-key algorithms are much slower than symmetric-key algorithms.

1.2 Cloud Computing

Frameworks for programming, middleware and application development platforms, and business applications are all examples of resources that may be shared in a cloud-based environment. Cloud computing's operating models, for example, include free infrastructure services with a value-added platform and subscription-based infrastructure services with an extra application service, among others. Cloud computing has been approached differently by diverse groups of people, including analyst firms, academics, business practitioners, and IT corporations. The cloud is a massive library of virtualized resources that can be accessed quickly and conveniently from any location with an internet connection. A broad variety of loads may be handled by resources that can be dynamically modified, enabling the most appropriate resource to be used at any given moment.

It's safe to say that it's the most talked about issue in the IT industry. Google, Amazon, Yahoo, IBM, Microsoft, and other online service providers, as well as many medium-sized businesses, are placing a great lot of emphasis on the cheap cost of the platform, which has become the primary focus of the company.

1.2.1 Benefits Of Cloud Computing

- Expand scalability: It is scalable on demand. Cloud computing has the flexibility to adapt to a user's changing needs. It is capable of increasing and managing resources.
- Less infrastructure costs: You don't have to spend any money on infrastructure since the service is based on a pay-per-use model. Cloud Computing allowed organisations to own their own storage and computing resources, based on their own requirements.
- Increase utilization: In cloud computing, several clients may share computer resources, resulting in a higher level of usage.

- Improve reliability: It is simpler to back up and restore data in the cloud than on a physical device since the data is kept in the cloud.
- Easy reach to resources: smaller firms previously couldn't afford to take use of cloud computing's more complex technologies. These resources are accessible over the internet since they are hosted in the Cloud.
- Easy Cloud Computing assemble: One may access the information in the cloud from any location with an internet connection after enrolling in the cloud.

1.2.3 Application of Cloud Computing

- In addition to development and testing, the client of the cloud may build and test their whole output on demand in the cloud environment. Because of the time and money saved in comparison to a conventional approach, developers may quickly transition from design to function. It also gives the patterns for iterative active development, the chance to test, and the ability to quickly move out a competitive advantage with the cloud.
- There are a number of options available for cloud-based spam and virus protection. Anti-spam sorting and antivirus services are two common functions of cloud services used by many enterprises. Even though the bulk of your organization's services are hosted in-house, they may be simply relocated to the cloud.
- IT Research and Education Educators and researchers may create their own programming models and application schedules using cloud computing since it enables numerous cloud deployment patterns (public, private, hybrid, or community), a variety of application programming models, and an extensible framework. Because of the cloud computing platform, the software industry is changing its focus from producing programmes for personal computers to data centres.

2. Literature Review

Mohd. Akbar (2021) Computing in the cloud is rapidly evolving into a powerful network architecture for large-scale and sophisticated computing tasks alike. An overview of cloud computing ideas, principles, current deployments, and research issues is presented in this paper. Data sent through the Internet is becoming more significant due to concerns about its security. In order to safeguard important files, we have come up with a strategy. Encrypting sensitive data using cryptography techniques is an effective method. A system of retrieval and transmission that can only be accessed by those who are supposed to utilise it. Cloud computing is helpful because of its cheap costs and ease of use. Cloud storage offers a number of benefits, including inexpensive costs and the ability to access data through the Internet. Cloud data security is critical because users often store sensitive information in cloud storage services, yet these services are not secure. When data is stored in an untrustworthy cloud, it remains a problem to securely interchange data. Using the AES, RC2 algorithm and a single cloud, our system protects and secures consumers' private data. As previously stated, the cloud computing idea and the transitional debate under cloud computing will be presented in detail. The most recent development in cloud security is discussed, as well as the cryptographic technique utilised in the cloud.

Bayan A. Alenizi (2021) As a service, dynamically scaled cloud computing (CC) solutions are made available through the Internet. Cloud computing is primarily motivated by the potential savings in both capital and operational costs that may be achieved by using cloud computing services. In order to make this a reality, there are still a few obstacles to overcome. Numerous researchers have solved security and privacy problems, yet the problem still persists. Adoption and expansion of cloud computing are both facilitated by a sense of security. This article presents a thorough examination of underlying cloud security and privacy problems and remedies in order to give a full understanding of current cloud security difficulties and mitigation solutions. As part of our study, we've developed a framework for addressing security and privacy problems in CC. When it comes to the protection of credit card data, the proposed architecture makes use of a hybrid authentication method. Researchers and practitioners may get a better understanding of CC and the underlying security and privacy problems, as well as countermeasures and a creative solution, thanks to this work.

Hossein Abroshan (2021) Cloud computing security is one of the most important concerns facing the cloud services business, and it is one of the most difficult to achieve. While it comes to providing secure and trustworthy cloud services, a robust encryption solution that has no or little impact on performance when working with data in a cloud environment is required. Cloud computing security has been improved by using a low-impact cryptographic technique, which has been developed by researchers. Because processing speed is crucial in cloud computing, a sophisticated cryptography method is not advantageous in this situation. The ellipticcurve-based methodology is utilised in combination with the Blowfish method since it has been significantly improved over the years. The use of Blowfish and the elliptic curve methodology will improve security and performance, respectively, as compared to other methods. In addition, a digital signature is used to ensure that the data is accurate and authentic. There is an increase in throughput, execution time, and memory utilisation while using this method of operation.

Gaurav Raj (2020) Cloud computing allows for resource expansion and dynamic development without the need for additional architecture, personnel, or software. Contrary to this, cloud computing was born out of a commercial need and has since flourished as an IT breakthrough. Despite the fact that the cloud houses a great deal of personal and commercial data, concerns have been raised concerning the cloud's security. Safety in cloud services, including data privacy, information security, virtualization security, software security, and access control, is by far the most important challenge. One of the most important issues here is one of privacy. The main reason for this is that organisations can only migrate their data to remote servers if cloud vendors guarantee assurances of data protection. It is possible for businesses and individuals to utilise programmes without setup and to see essential documents on any Wi-Fi access device through cloud storage. In cloud computing, the data will also be stored by the cloud service provider. Cryptography, which offers encryption mechanisms in a computer environment to safeguard information and processing, is one of the main focuses of the article. Cloud computing Modern encryption is a safe and secure way to safeguard your data in the cloud.

Bhargav, A. &Manhar, Advin (2020) Rather of using a proprietary disc drive or local memory device, cloud computing delivers computing services via the internet. Servers, storage, databases, networking, and software are all examples of computing services. The cloud's primary benefit is that users may access and store data on the cloud from any location at any time, and they can do so at a minimal cost. In spite of this, cloud computing's lack of direct client involvement has made security a major issue for many users. It is doubtful that cloud computing service users are aware of how their data is being transported when they upload or save data. Third parties may or may not have access to the user's information. The user is unaware of this. Various cryptography algorithms have been developed to address security concerns. A review of current cloud computing cryptography techniques was the primary objective of this article.

3. Objectives of the Study

- to study Cryptography Techniques In Cloud Computing And Their Role And Applications
- to analysis the securing cloud storage data using multi-level encryption and decryption

4. Research Methodology

Secondary data was gathered for this study from several web sources, academic journals, and the Google Search Engine.

4.1 *Security Issues*

There are several interconnected networks that make up cloud computing. One of the risks connected with the cloud is that an unauthorised individual might get access to your data. While data is being sent, it may be intercepted and altered by a third party. Data integrity, availability, confidentiality, privacy, and control over where data sits are all major concerns when it comes to cloud data security. Data security may be achieved in a variety of ways, including via the use of access restrictions and encryption. It is the responsibility of the client to learn more about the data security measures offered by the cloud provider and how they are implemented.

5. Existing Algorithms

1. Des (Data Encryption Standard)

DES is a symmetric block cypher invented by IBM and is still in use today (Data Encryption Standard). DES is an implementation of the Feistel Cipher. A Feistel structure with 16 rounds is used. The block size is set to 64 bits by default. DES's key length is 56 bits, which is an efficient amount considering that only 8 of the key's 64 bits are actually used by the encryption process. The following illustration demonstrates how DES works.

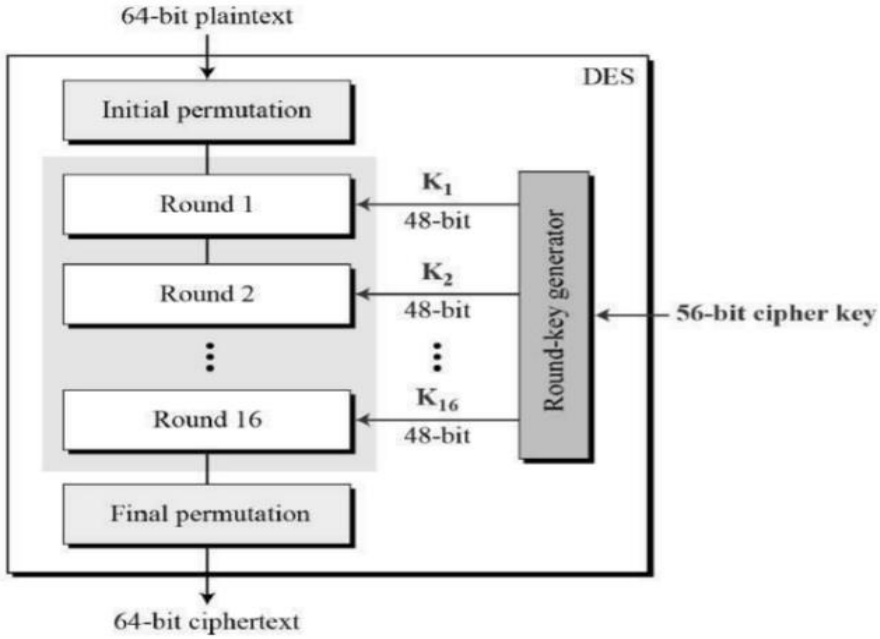

Fig:1Description of DES Algorithm

The DES trifecta (3DES) In order to employ 3TDES, the user must first develop and then distribute a 3TDES key K, which comprises of three separate DES keys (K1, K2, and K3). This indicates that the Triple DES key has a length of 356 = 168 bits. The encryption method is shown in the following manner:

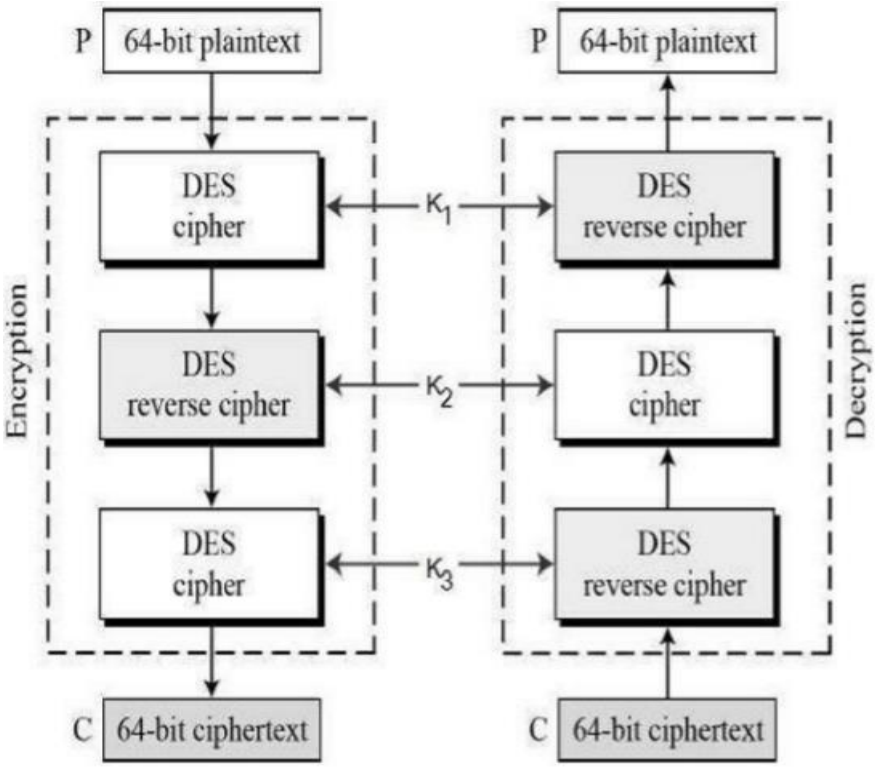

Fig:2 Encryption Procedure

The encryption-decryption process is as follows

- Encrypt the plaintext blocks of data using single DES with key K1.
- Now decrypt the output of encrypted data in Step 1 using single DES with key K2.
- At this step, encrypt the output of step 2 using single DES with key K3.
- The output obtained after step 3 is the final cipher text.
- The inverse procedure is the decryption of a cypher text to plaintext. Encryption occurs initially with K3, followed by decoding or decryption with K2, and then decryption with K1.

2. Rsa Algorithm

For public-key encryption, one of the most widely used and safest algorithms is RSA (Rivest-Shamir-Adleman). This technique was created because factoring huge integers is very difficult. This algorithm's operation is described in the following way, using an encryption key (e,n):

1. Use an integer number from 0 to 1 to represent the message (n-1). Many blocks may be used to break down very big messages. The equivalent number in the same range would then be assigned to each block.
2. Raise the plaintext message to the eth power modulo n and encrypt it. C is the ciphertext message that is generated.
3. Raise the encoded message C's power d modulo n to decode/decrypt it.

Publication of the encryption key (e,n) It is the user's responsibility to protect the decryption key (d,n).

Calculate the Values for e, d, and n

1. Choose any two very large (100+ digit) prime numbers. Represent these numbers as p and q.
2. Set n equal to p * q.
3. Choose any large integer, d, such that GCD (d, ((p-1) * (q-1))) = 1
4. Find e such that e * d = 1 (mod ((p-1) * (q1)))

It is impossible to verify the security of cryptographic techniques. The RSA method of attaining security relies on the fact that factoring huge integers is exceedingly difficult. n is about 200 digits long if p and q are higher than 100-digit values. The attacker will have a tough time factoring the numbers. Other approaches to figuring out d that don't include factoring in n are just as challenging. Any cryptographic algorithm that is able to withstand a severe assault is considered secure. The RSA algorithm is deemed safe at this level.

6. Comparison

Secret keys and public keys are used to compare the DES and RSA algorithms, and the results are presented in a table. With RSA, the problem of key agreement and exchange in secret key cryptography is made simpler to solve. It does not, however, handle the whole security architecture in its entirety. In this instance, DES is the industry standard. RSA and DES have properties that are distinct from one another. In comparison to other encryption techniques, the throughput and power consumption of DES are both much higher. Issues with key distribution and agreement are two of the most prominent drawbacks of DES algorithms, according to the literature. RSA techniques, on the other hand, need a significant amount of

time to complete both the encryption and decryption processes. According to the findings of a simulation, DES surpasses RSA in terms of security. In comparison to the RSA technique, it is believed that the DES algorithm has a greater throughput. As a consequence, due to the triple phase structure of 3DES, it consumes more power and has a poorer throughput than the DES. In practise, it has been shown that decryption using the DES algorithm is both quicker and more energy efficient than alternative approaches.

DES and RSA are used for encryption and decryption when data is downloaded from Cloud Storage, which allows me to overcome the limitations of these two methods while simultaneously making more use of each. This approach is being used to improve security, and I'm hoping to publish it soon. This suggested solution will only safeguard text files, and no other types of data will be protected. The technique is designed to achieve the following objectives while simultaneously increasing the security of data storage.

1) For Encryption of text files:
- ♣ Upload plaintext file to encrypt.
- ♣ Apply DES algorithm of Encryption to generate first level encryption.
- ♣ Apply RSA algorithm of Encryption to generate second level encryption.
- ♣ Store Cipher Text into Database.

2) For Decryption of text files:
- ♣ Read Cipher Text from Database.
- ♣ Apply RSA algorithm of Decryption to generate first level decryption.
- ♣ Apply DES algorithm of Decryption to generate Plain text.
- ♣ Display Plain Text to User.

7. Conclusion

The use of cryptography in the cloud Crypto Cloud Computing is a brand-new, secure cloud computing architecture. In addition to securing system-level information, it enables users to access shared services quickly and correctly. People's networks are protected by crypto cloud computing. It is able to guarantee the privacy of a person without any delay in the sharing of information. The DES algorithm is used to generate the first level of encryption in our proposed system. The DES algorithm's encrypted output is then subjected to a second round of encryption using the RSA method. Both DES and RSA methods are decrypted in the same way, although in reverse order. The term "multilevel encryption and decryption" describes the method we used to protect the data in our cloud storage system. Users may access cloud computing resources and services over the internet, provided by cloud service providers, at any time and from any location. The fact that every enterprise is moving its data to the cloud implies they are relying on the storage services offered by the cloud provider. As a result, several assaults on that data must be guarded against.

References

[1] Mohd. Akbar.(2021). Study and improved data storage in cloud computing using cryptography. International Research Journal on Advanced Science Hub (IRJASH). Volume 03 Issue 02S February 2021

[2] Bayan A. Alenizi.(2021). Security and Privacy Issues in Cloud Computing. International Conference on Recent Trends in Computing (ICRTCE-2021). Journal of Physics: Conference Series 1979 (2021) 012038

[3] Hossein Abroshan.(2021). A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6, 2021

[4] Gaurav Raj.(2020). Use of Cryptography in Cloud Computing for Enhancing the Security. JOURNAL OF CRITICAL REVIEWS ISSN- 2394-5125 VOL 7, ISSUE 10, 202

[5] Bhargav, A. &Manhar, Advin. (2020). A Review on Cryptography in Cloud Computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 225-230. 10.32628/CSEIT206639.

[6] Dickson KodzoMawuliHodowu.(2020). An Enhancement of Data Security in Cloud Computing with an Implementation of a Two-Level Cryptographic Technique, using AES and ECC Algorithm. International Journal of Engineering Research & Technology (IJERT). ISSN: 2278-0181. Vol. 9 Issue 09, September-2020

[7] Zaineldeen, Samar & Ate, Abdelrahim. (2020). Review of Cryptography in Cloud Computing. 9. 211-220.

[8] Mizyad, Wissm. (2020). CRYPTOGRAPHY IN CLOUD COMPUTING FOR DATA SECURITY AND NETWORK SECURITY. 63. 6965-6973.

[9] Sharma, Shantanu &Burtsev, Anton & Mehrotra, Sharad. (2020). Advances in Cryptography and Secure Hardware for Data Outsourcing (IEEE ICDE 2020). 1798-1801. 10.1109/ICDE48307.2020.00173.

[10] Dharmakeerthi, Thilina. (2020). A Study on Secure File Storage in Cloud Computing using Cryptography (April 2020).