International Journal of Research in Engineering, Science and Management
Volume 5, Issue 5, May 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Secure File Storage on Cloud Using a Hybrid Cryptography Algorithm

Samson Michael Khamis Wani[1*], Abhay Kumar[2]
[1,2]*Bachelor of Computer Applications, Department of Computer Science and Engineering, Galgotias University, Greater Noida, India*

Abstract*: In recent times most people and firms are migrating to the cloud due to the fact the cloud is much less luxurious and handy. For some pc owners, locating sufficient storage space to keep all the statistics they obtained is an actual undertaking. Because of this, humans tend to shop for a huge quantity of facts or large space hard drives and are nonetheless confronted with storage area demanding situations. With this new era of cloud computing, people are finding it a great deal easier to buy a large quantity of space on the cloud, this cloud refers to saving facts to an off-off-website garage system maintained via a third birthday celebration. Due to a majority of these, cloud users start considering the protection of their information stored on those servers managed with the help of a third party the fear of records Breach. Facts protection is wanted to curtail this statistics breach and lots of information threats. Cryptography performs a main position in records security. To offer security to cloud storage, users use hybrid encryption in place of a single encryption algorithm. A hybrid cryptosystem combines the ease of a public-key cryptosystem with the performance of a symmetric-key cryptosystem. Public-key cryptosystems are handy in that they do not require the sender and receiver to proportion a commonplace secret to speak securely. However, they often depend on complex mathematical computations and are therefore commonly a great deal extra inefficient than similar symmetric-key cryptosystems. In this proposed machine 3DES (Triple information Encryption trendy), RC6 (Rivest Cipher 6), and AES (Advanced Encryption popular) algorithms are used to provide safety to records. All of the algorithms use 128-bit keys. LSB steganography technique is used to securely shop the important thing facts. Key data will contain information concerning the encrypted part of the file, the algorithm, and the algorithm's key. File throughout encryption is cut up into three components. These character parts of the report may be encrypted with the use of one-of-a-kind encryption algorithms concurrently with the assistance of the multithreading technique. The important thing to record inserted into a photograph is the usage of the LSB approach. Our technique guarantees better safety and protection of purchaser statistics by storing encrypted data on a single cloud server, and the usage of AES, DES, and RC6 algorithms.

***Keywords*: Defining cloud and cloud computing, data protection on the cloud, hybrid cryptosystem, AES algorithm, AES cipher, 3DES.**

1. Introduction

This task goal is to build an end-to-end-to-quite encrypted at ease file storage machine the use of, which users can securely share documents with different users. Customers can save any sort of record like textual content documents, audio documents, photographs, etc. The device calls for a report as input this is then encrypted with the use of cryptography techniques and saved at a far-off location.

Cloud computing is a paradigm of computing and a brand-new way of considering the IT industry. It isn't any unique technology and due to its evolving nature, its definition is also evolving.

Cloud computing is a type of parallel and distributed machine inclusive of a group of interconnection and virtualized computers that can be dynamically provisioned and presented as one or greater unified computing assets based on a service level agreement (SLA) installed through negotiation between the carrier provider and purchasers.

In Cloud computing documents and software aren't completely contained in the person's application, and programs live on company premises. The cloud provider can clear up this problem by using encrypting the documents via the usage of an encryption set of rules. This paper offers a report protection model to offer an efficient answer for the basic hassle of safety in cloud surroundings. In this model, hybrid encryption is used in which documents are encrypted via file splitting, and RSA is used for secured communication between customers and the servers.

Defining a cloud:

Cloud computing has become a popular buzzword and it has been broadly used to consult exclusive technology, services, and concepts.[4] "It's far regularly related to virtualized infrastructure or hardware on-call for, software computing, IT outsourcing, platform and software as a service, and many different matters that now are the focal point of the IT enterprise" [4].

The period "cloud" has historically been used inside the telecommunication enterprise as an abstraction of the network in device diagrams. It then became the image of the most famous computer community: The net. This meaning also applies to cloud computing, which refers to an internet center's way of doing computing. The internet plays an essential position in cloud computing because it represents either the medium or the platform thru which many cloud computing services are added and made reachable.

*Corresponding author: samsnmichael@gmail.com

Cloud:

A cloud is a kind of parallel and distributed machine inclusive of a group of interconnected and virtualized computer systems which are dynamically provisioned and offered as one or more unified computing assets primarily based on carrier-level agreements mounted through negotiation between the carrier provider and consumers.

Cloud computing:

Cloud computing is a model for enabling convenient, on-demand communities to get entry into a shared pool of configurable computing resources (e.g., Community, servers, garage, packages, and offerings) that may be hastily provisioned and launched with the minimum, management, and attempt, or carrier company interaction. [4]" Additionally, we virtually positioned, cloud computing as the delivery of computing offerings—inclusive of servers, garage, databases, networking, software program, analytics, and intelligence over the net ("the cloud") to offer quicker innovation, flexible resources, and economies of scale" [4].

From the definition provided above and from the fundamental standards furnished about cloud computing, it could be concluded that the significant thoughts at the back of cloud computing are as follows.,

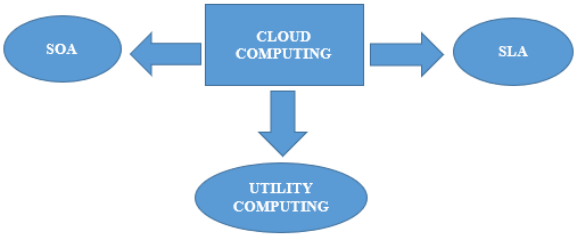

Fig. 1. Central ideas behind cloud computing

- utility computing
- SOA – Service-Oriented Architecture
- Service Level Agreement

This combination of application computing, SOA, and SLA affords scalability, elasticity, availability, reliability, manageability, interoperability, performance optimization, and accessibility portability, these functionalities serve users in severe approaches.

Types of Cloud Computing:

There are many types of cloud computing, below are the main three types,

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Software as a service (SaaS)

SaaS is a shape of cloud computing in which customers can access software applications without needing to download, deploy, or keep that software program and its various components on their gadgets or tough drive. Most cloud computing software of this type is subscription-based with an annual or monthly rate. In return, customers get seamless answers and functions without having hardware, being slowed down using installing updates, or other preservation tasks.

When it was founded, Salesforce changed into one of the first cloud computing and SaaS groups. Its income Cloud, advertising Cloud, and provider Cloud are all cloud-based software applications.

1) Platform as a Service (PaaS)

Platform as a provider (PaaS) is a cloud computing solution that provides developers with a smooth-to-use platform to create their software, web packages, or different programming tasks. Businesses use PaaS to create proprietary apps and applications without the want for servers or special testing environments.

Salesforce has been within the PaaS market for over a decade and is the leader in the organization PaaS. The Salesforce Platform gives companies the electricity to build apps and offerings with Heroku organization, private spaces, Salesforce Lightning, and Trailhead. The platform's versatility lets developers put in writing code within the language of their choice. It integrates with other cloud computing merchandise that uses purchaser information, allowing organizations to the song an app's performance.

2) Infrastructure as a Service (IaaS)

Infrastructure as a carrier (IaaS) gives organizations with getting entry to servers, firewalls, digital machines, storage, and different infrastructure. It's ideal for organizations that create especially specialized or particular proprietary packages, but don't want to spend time or other sources buying, storing, setting up, or keeping the necessary equipment. Rather, they get the right of entry to prepared-to-use infrastructure over the internet.

Data security problems:

Cloud Computing is a type of era that provides far-off offerings on the internet to control, get admission to, and store data instead of storing it on Servers or local drives. This generation is likewise referred to as Serverless technology. Right here the data can be whatever like snapshots, audio, video, files, documents,

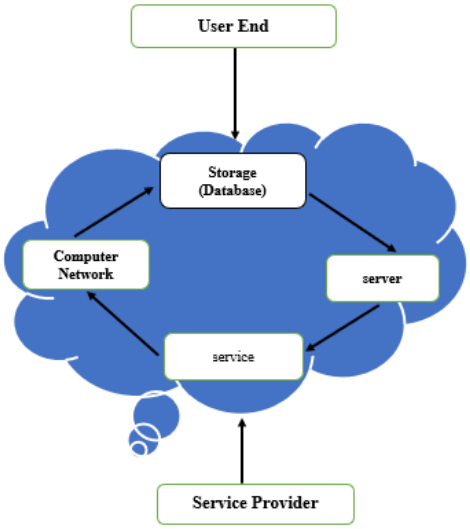

Fig. 2. cloud security

There is no doubt that Cloud Computing provides numerous benefits but there also are a few protection troubles in cloud

computing. Under are some following safety troubles in Cloud Computing as follows.,

Data loss:

Data Loss is one of the problems faced in Cloud Computing. This is also referred to as facts Leakage. Our sensitive information is in any individual else's arms, and we don't have complete management over our database. So, if the safety of cloud services is broken by using hackers, then it could be feasible that hackers get access to our touchy data or private files.

Interference of Hacker in insecure APIs:

[1] "As we realize if we're speaking approximately the cloud and its services it's why we're talking approximately the internet. Also, we recognize that the very best way to communicate with Cloud is the usage of API.so it's miles critical to shield the Interface and APIs that are used by an external user. However additionally in cloud computing, few services are to be had inside the public area. That is the vulnerable part of Cloud Computing because it may be possible that those offerings are accessed via a few third parties. So, it could be feasible that with the help of those offerings hackers can without difficulty hack or damage our statistics (Data) [1].

User Account Hijacking:

Account Hijacking is the most critical security difficulty in Cloud Computing. If someway the Account of a person or an organization is hijacked by way of a Hacker. Then the hacker has complete authority to carry out Unauthorized activities.

Changing Service Provider:

Dealer lock-in is also an important security problem in Cloud Computing. Many groups will face one-of-a-kind troubles at the same time as shifting from one supplier to another. For instance, A business enterprise desires to shift from AWS Cloud to Google services. They ace diverse problems like shifting all data. Each cloud services have one-of-a-kind techniques and capabilities, so in addition, they face issues concerning that. Also, it could be possible that the expenses of AWS are specific to Google Cloud and many others.

Lack of Skill:

Whilst working, moving on to every other service provider, desiring a further function, how to use a function, and many others. These are the main issues due to an IT organization that doesn't have a professional worker. So, it requires professional cloud Computing.

Denial of Service (DoS) attack:

This kind of attack takes place whilst the machine receives too many visitors. DoS assaults arise in huge corporations which include the banking area, authorities' zone, and so on. When a DoS assault occurs, information (Data) is lost. Improving each record requires the sum of money in addition to time to address such issues.

Hybrid Cryptosystem future action:

The hybrid Cryptography concept is used for securing the storage device of the cloud. Extraordinary processes are used to show the distinction between less comfortable and greater comfortable structures. The first approach makes use of RSA and AES algorithms; RSA is used for key encryption and AES is used for text or statistics encryption. Inside the 2d or we can say a more secured approach, AES and Blowfish algorithms are used. In this method, those two algorithms offer double encryption over statistics and keys which gives high protection in comparison to the primary one.

- On this proposed device 3-step approaches are used. First of all, Diffie Hellman is used for changing keys. Thereafter authentication is done using a virtual signature scheme. In the end, facts are encrypted with the use of AES and then uploaded to the required cloud device. For decryption, a reverse procedure is applied.
- Mixture of RSA algorithm and MD5 to assure numerous safety features along with confidentiality, data integrity, no repudiation, and so forth. It uses the RSA key technology set of rules for the technology of encrypted keys for the encryption and decryption manner. The MD5 digest is used for accepting an input of duration up to 128 bits and processing it and producing an output of a padded period for the encryption and decryption system.
- Implementation of trusted garage gadget the use of Encrypted report gadget (EFS) and NTFS record device power with the assistance of cache supervisor for securing facts documents. EFS encrypts stored documents by way of routinely using cryptographic systems. The method takes region as follows, firstly the application writes documents to NTFS which in flip places them in cache and returns them to NTFS. After this NTFS asks EFS to encrypt documents and heads them closer to the disk.
- Cloud garage safety provider is supplied using separate servers viz. Consumer input, information storage, and user Output. Three specific servers are used to ensure that the failure of any of the servers doesn't harm the data. The consumer enter server is used for storing personal documents and entering facts using providing consumer authentication and ensuring the records aren't always accessed via any unauthorized means. The information garage server is the area where the encryption using AES is performed to comfy person input and then the encrypted documents are transferred to the user Output server. User Output Server is the place from where the user receives the output record or the decrypted report and makes use of it for similar use.

Advanced Encryption Standard (AES):

The advanced encryption Standard (AES) is called Rijndael encryption. Rijndael is a block cipher followed as encryption well known using the U.S.A government. AES was announced via the countrywide institute of preferred and era (NIST) on November 26, 2001 aa after a 5-years standardization procedure.

AES is one of the most popular algorithms utilized in symmetric key cryptography. It is available by way of desire in many different encryption applications. The cipher become advanced using Belgian cryptography cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES choice technique beneath the name "Rijndael".

[2] In contrast to DES, its predecessor, Rijndael is a substitution-permutation network, not a Feistel community. AES is speedy in each software and hardware, is especially easy

to put in force, and calls for little memory. As new encryption is popular, it's far presently being deployed on a large scale.

AES is not precisely Rijndael (even though in exercise they're used interchangeably) as Rijndael supports a larger variety of block and key sizes; AES has a fixed block length of 128 bits and a key size of 128, 192, and 256 bits, whereas Rijndael can be unique with key and block sizes in any more than one of 32 bits, with not less than 128 bits and a maximum of 256 bits.

Because of the fixed block size of 128 bits, AES operates on a 4x4 array of bytes, termed the nation (variations of Rijndael with a huge block size have extra columns inside the nation). Most AES calculations are accomplished in a special finite subject.

AES is founded on the strong and properly-posted mathematical ground and looks to withstand all recognized attacks properly. There's a strong indication that no back-door or acknowledged weak spot exists since it has been published for a long term, has been the situation of excessive scrutiny using researchers all over the international, and has such sizeable amounts of financial v, the cost changed into deceased with the aid of Belgian researchers in Belgium, therefore, voiding the conspiracy theories from time to time voiced regarding an encryption well-known advanced by the U.S. Authorities corporation. A robust encryption set of rules want handiest a single principal criterion:[2]

- There must be no way to find the unencrypted clear text if the key is unknown, except brute force to try all possible keys until the right one is found.
- The number of possible keys must be so large that it is computationally infeasible to stage a successful brute force attack in a short enough time.

The older standard, Date Encryption Standard (DES) meets the first criterion, but is no longer the secondary one computer speeds have caught up with it, or soon will. AES meets both criteria in all of its variants: AES-128, and AES-256.

AES cipher:

The AES cipher is special as several repetitions transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds is applied to transform ciphertext back into the original plaintext using the same encryption key.

Triple Data Encryption Standard (3DES):

In cryptography, 3DES is an inherited more advantageous version of DES (records Encryption trendy). In the Triple-DES set of rules, DES has been used twice to grow the security stage. Triple DES is also known as TDES or Triple records Encryption algorithm (TDEA).

TDES has the following keys:

- All keys are different.
- Key 1 and 2 are different & key 1 and key 3 are the same.
- All keys are identical.

Triple-DES with three keys is pretty simple to apprehend. Triple DES with 3 keys uses 3 keys k1, k2, and k3. It first plays the DES Encryption process at the authentic plaint the use of key K1 to get the ciphertext (say C1). Now it plays the DES decryption process on the Ciphertext (C1) however this time with the second key K2 to get the text p1. Now again performs the DES Encryption process at the text (p1) however this time with the third key k3. The very last output is the ciphertext.

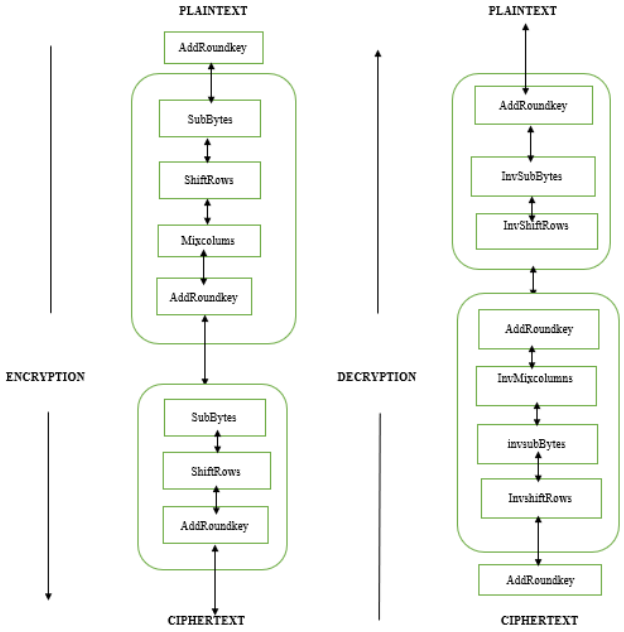

Fig. 3. Encryption/Decryption process of AES

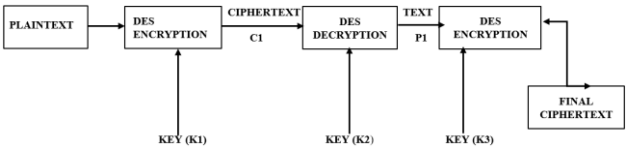

Fig. 4. Triple data encryption standard with 3 keys

A) User Registration

For getting access to the offerings, the user ought to first check-in himself. All through the registration manner, numerous facts like call, username, password, electronic mail identity, and the smartphone quantity can be asked to enter. Using this information the server will produce unique person-precise keys to be used for encryption and decryption purposes. However, this key will not be stored within the database instead it will be stored the use of the steganography algorithm in a picture as a way to be used as the person's profile picture.

1) Uploading a File on Cloud

- Whilst the person uploads a record/ file on the cloud-first it is going to be uploaded in a transient folder.
- Then user's document will be cut up into N elements.
- These elements of the document may be encrypted using cryptographic algorithms. Every part will use an extraordinary encryption algorithm.
- All components of the document might be encrypted using specific algorithms which might be AES, 3DES, and RC6. The key to those algorithms could be retrieved from the steganographic photo created at some stage in the registration.

- After the cut-up encryption, the record is reassembled and saved in the person`s precise folder. The original record is eliminated from the transient folder.
- Then gather all Encrypted components of the file.

B) Download a File from the Cloud

- Whilst the consumer requests a report to be downloaded first the report is broken up into N parts.
- Then those parts of the file will be decrypted using the equal algorithms with which they had been encrypted. The key to the algorithms for the decryption procedure may be retrieved from the steganographic photo created all through the registration.
- Then those components might be re-blended to shape a fully decrypted record.
- Then a document will be dispatched to the person for download.

2. Conclusion

The main target of this system is to safely store and recoup data on the cloud that's only controlled by the proprietor of the data. Cloud storage problems of data security are answered using cryptography and steganography ways. Data security is attained using RC6, 3DES, and AES algorithms. Crucial information is efficiently stored using the LSB fashion (Steganography). less time is consumed for the encryption and decryption process using the multithreading fashion. With the help of the proposed security medium, we've fulfilled better data integrity, high security, low detention, authentication, and confidentiality. In the future, we can add public-crucial cryptography to avoid any attacks during the transmission of the data from the customer to the server.

References

[1] Uttama Kumar, Jay Prakash. “Secure file storage on cloud using hybrid cryptography algorithm,” International journal of creative research thoughts, July 2020.
[2] Vikas Chaudhary, Kanika Garage, “Cryptography and network security.”
[3] Arjun Kumar, Byung Gook Lee, Hoonjae Lee, “Secure storage and access of data in cloud computing,” Anu Kumari, Busan, 617-716, Korea, 2012.
[4] Rishabh Sharma, “Cloud computing, fundamentals, industry approach and trends, Wiley India, 2015,
[5] Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi, “Mastering cloud computing,” McGraw Hill Education.