WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Enhance Cloud Data Protection using Anonymous Encryption

Sharik Ahmad and Ms. Sneha Deokate

Department of Computer Science and Engineering
School of Research and Technology, People' University, Bhopal [MP], India

A B S T R A C T

Online social networks have become the standard in recent years. Social media networks allow users to communicate with their family, friends, and colleagues. Data published on social networks and other forms of media spreads rapidly and thoroughly, making it enticing to attackers to gain information. Community networking environments may not come without risk. There are several security and privacy concerns with the user's shared information, particularly when the user uploads personal content like photographs, videos, and audios. Data security is a key issue in the cloud. Data security in this context refers to the theft of data by attackers. These AES algorithms ensure data security in an effective manner. The first module employs an anonymization mechanism in conjunction with an advanced encryption standard algorithm. Anonymization is an alternate encryption method. The input data is anonymised and stored in some format on a cloud server. The anonymized output is the plaintext input to the AES algorithm. The AES algorithm encrypts the input once again and returns some ciphertext output. This ciphertext data is dynamically saved in the cloud server. The total execution time is lowered by 0.6%. However, CPU consumption has increased by 0.2%. The level of security has been raised. The supplied data is simulated and improved using the Cloudsim program. Overall execution time is lowered by 34%. This proposed approach yields superior results for secure data in a cloud setting.

Keywords:Cloudsim, encryption, AES, Data security

1. Introduction

Cloud computing is a fast computation technique that makes use of centralised storage, memory, processing, and bandwidth. The internet and a central remote server aid in the maintenance of data and applications. Cloud computing is a service that is provided on a subscription basis. By using a cloud service, one can connect to any application from anywhere and access shared resources, software, and information for a fee. Virtualization in computing refers to the version of software, hardware, and network resources.

Cloud computing establishes a trend of extracting values from delivery services while increasing speed and integrity. It reduces the time required to create an application product to real preparation. Cloud computing includes visualisation, on-demand deployment, internet processes, computing utility delivery, and open source software. The servers provide a pool of resources that may be managed as needed, as well as the relationship of applications to computation or storage. As virtualization enables a dynamic data centre, network resources change regularly to meet each workload and business requirement.

2. Objective of the Research

The primary goal of the work is to improve cloud data security while also protecting user data. Advanced Encryption Standard algorithm is one among the best algorithm in encryption method. Anonymization is used as an alternative method for data encoding process. The proposed method is to hybrid these two techniques named as Anonymizaion with AES algorithm.

3. Computer and Data Security

Data is a set of values and variables. These data are made up of some human-readable information. Data is transformed into digital data with the construction of a computer system. In digital data, information is turned into binary 0s and 1s. This binary format is saved on the computer. In this case,

E-mail address: shariqahmed180@gmail.com

data includes not only text but also image, audio, and video files, which are translated into binary format. Previously, data was saved on magnetic tapes and floppy diskettes. Data is currently stored in hard drives, either internal or external.

The data processing life cycle is depicted in Figure 3.1. The user's data will be gathered and sent to the processing unit. The data is processed by the processing unit based on the needs of the user. After the processing unit is finished, it moves on to the output and storage units. This data might be saved in a cloud server using current computing technology. A computer-based data processing system is made up of both software and hardware. It will generate a dependable and input-based processing system.

The data is saved in a computer, and its security must be verified. Users anticipate greater security and privacy for their data. As a result, the phrase security has gained significance in our country. Data security refers to the complete process. The primary function of this data security approach is to protect computer hardware and software systems. Data security safeguards user data and ensures privacy. Only authorised people have access to and can change the data.

In the electronic data storage procedure, information communication technology is implemented. The goal of this ICT is to modernise data processing by incorporating new technology. The internet is the backbone of ICT since computing technology cannot be implemented without it. ICT is used in both the public and private sectors. The goal of data security is to keep data loss to a minimal. More than 99% data security will be maintained. Hackers develop innovative techniques to hack data. Every incidence contributes to the improvement of data security. They require some policy and practise to ensure data security.

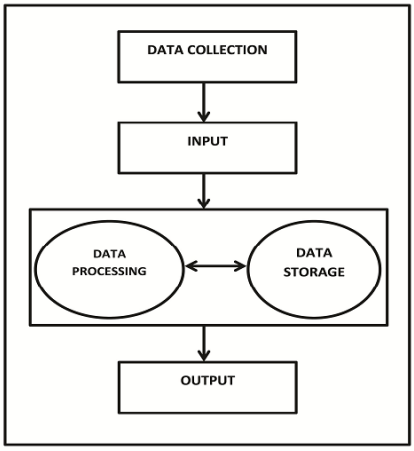

Figure 3.1Data processing life cycles

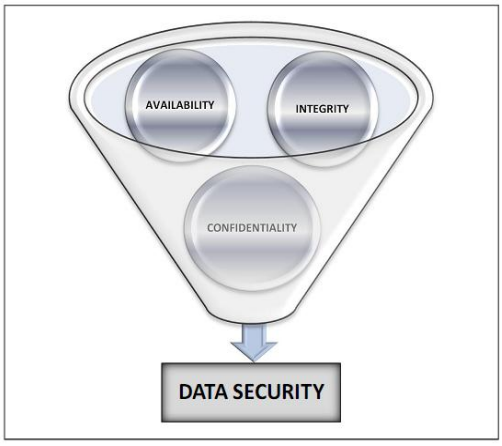

Figure 3.2Data Security

3.1. Aim of Data Security

The primary goal of data security is to provide the highest level of protection for individual and organisational data. The secondary aspect of data security is minimising risk and increasing user security. Figure 3.2 depicts the elements of data security.

Confidentiality: - The confidentiality system is comparable to the privacy system. The primary objective of confidentiality is to protect highly sensitive information. The correct individuals receive the proper information. The user account number and password for the banking and financial industry are critical. This information will be encrypted and then processed. In this instance, the biometric verification method is sometimes utilised to administer the user account.

Integrity: - The goal of data integrity is to keep data accurate and consistent throughout the data processing process. They guard against unauthorised data access and manipulation. Hackers attempt to alter the user's information. They identify the process of data alteration and notify the administrator. Even if this integrity verification is used, the data may go through a checksum and encryption process.

Availability: - Data availability is an important aspect of data life cycle and data security. The term "availability" refers to the ability to keep data available when a user requests it. The user may send a request to the server due to a system hardware fault. In this case, the special programme detects the malfunction and saves the data. It ensures proper data access and maintenance bandwidth. Because of the data disaster, they keep an additional server to keep the full data. This is referred to as data replication. This server is used when there is a data failure or loss.

The data security level is mainly classified into three types first one is Low, second one is Medium and third one is high. The data send from one terminal to other terminal has lot of attacks in network transmission. To avoid these issues mainly two types of implementation is suggested. One is software-based protection and another one is hardware-based protection. Installing antivirus and firewall software to protect the system files and operating system is software-based protection. Some operating systems include a unique firewall to protect against data hacking. Hardware protection involves the installation of firewall devices throughout the entire network. To ensure data protection, banks and financial institutions deploy hardware-based security devices. Hardware equipment is more expensive than software security systems.

Table 3.1 Security level Comparison

Security Levels	Confidentiality	Integrity	Availability
Low	0 to 49	50 to 79	80 to 100
Medium	0 to 49	50 to 79	80 to 100
High	0 to 49	50 to 79	80 to 100

Table 3.1 depicts security measurement and percentage levels. The low security level has little effect on ordinary data security. This will keep all security measurements between 0 and 49 percent. The medium security level has a high negative impact. This will have an impact on the entire organization's workflow, affecting both employees and service providers. High-level data security is critical; this will harm highly sensitive data.

3.2. Cloud Data Security Issues

Cloud security encompasses a wide variety of technology and data security. This will be related to several security domains such as network, computer, and information security. Corrective control, detective control, preventative control, and deterrent control are all sorts of cloud security controls. This rule prevents data theft and ensure cloud data security.

4. Research Methodology

The primary goal of cloud computing is the online sharing of software and hardware resources. Some steps have been taken to make sense of the above remark, but there are still some problems to be overcome in the domain of cloud networking. The most significant difficulty that providers and customers confront in the cloud environment is security. Some of the key benefits of cloud technology are lower costs and resource re-provisioning. To secure online documents, a common encryption method is utilized, and the characteristic that may suit well with security demands in the cloud environment is discovered.

4.1. K-Anonymity

Cloud computing is beset with a slew of data security issues. There are numerous approaches for data security. Anonymization is one of the most effective data security solutions. This method is widely utilized in the public cloud environment. The fundamental procedure of this anonymization technique is to change the data utilizing the data set's identity information. The identification of keys is critical in cloud data security. Any format will interchange or convert the original data. One strategy for anonymization is k-anonymity. The data will be divided into attributes and k-1 will be used. The value of the property should be increased or decreased. They select more reliable data from the data pool. For example, the health-care industry deals with various attributes in similar variables. Similar information, such as date of birth and gender, is repeated. Table 4.1 depicts the many types of k-anonymity.

Table 4.1 K-Anonymity Attribute Comparison

Attribute	Working Method	Example
Key	It will be working ondirect identification	Name and Aadhar CardNumber (Unique Number)
Sensitive	The user personal sensitiveinformation	Heal record, Banking Detail
Quasi-identifier	Data linked with external information	Data of Birth, Zip code and gender

The k-anonymity is used to change the data methods and property. The key attribute means direct indication of the user detail. The name and aadhar number are the unique identity of the user. It does not change the particular table. Second attribute is sensitive information; it maintains the user personal details like bank account number and personal health problem data. The third attribute is Quasi-identifier; it will be linked with some external data agency. It is not possible in unique data because same date of birth is there in many users. The last value of data changes some time, for example user age is 35 it will be changed 3*. The similar example for zip code 625634, it will be changed 625 ***. Last three digits will be hidden. This type of data changes is used to avoid the data attacks. The hacker try to hack the user information, they did not get the original information, because the original information is changed using this anonymization technique.

There are various approaches for anonymization. The first is data concealing, which is used in a specific field. For example, the user's monthly income field conceals the specific record. The following method is hashing, which is hashed in many fields such as user name and unique address. The permutation method assigns new values to old values. Adding some value to a specific field and mapping a single person's data to two other fields. The crap is a commonly used method for rounding a value added to a field, like as adding a value to the overall income field. These are the most widely utilized methods for data security in this publication. To safeguard cloud data, the proposed hybrid anonymization method and AES encryption algorithm are utilized.

4.2. Advanced Encryption Standard Algorithm

The formal encryption approach that has been generally used is known as Advanced Encryption Standard (AES), and it has been authorized by the US Government's National Institute of Standards and Technology. The algorithm is known as the symmetric-key algorithm, which is described by AES, and it uses the same key for both encrypting and decrypting data. The Rijndael algorithm is commonly known as the AES encryption algorithm. A block cipher is an advanced encryption method that works on single data blocks. The block cipher performs several rounds of encryption using the encryption key. The standard length of the AES encryption algorithm is 128 bits, or 16 bytes. To authenticate any user, the system's encryption and decryption processes are

insufficient. The aforesaid issue is addressed in the suggested system, which achieves high levels of security and performance through the use of AES with the Verify-Confirm-Update approach. The user is obtained and verified using a secret key method (anomaly and AES). The proposed VCU technique consists of three basic processes.

The proposed module describes key generation. When a user is authenticated, the server creates unique keys for the user to enter the cloud system. This instances generator generates the secret key using an AES key generator. This is produced and communicated to the cloud client via the LAN Wi-Fi connection key. This is received and copied for the purpose of decryption. As a result, the client can securely receive the requested file via the LAN connection. Rijndael algorithm in Advance Encryption Standard (AES), which is a symmetric method, delivers improved computing efficiency due to its simple operation and efficient execution.

As a symmetric-key block cipher, the National Institute of Standards and Technology (NIST) published the Advanced Encryption Standard (AES). The three major areas of security are as follows. The AES algorithm is distinguished by its low cost and ease of implementation. This is the primary reason NIST chose the AES algorithm. AES encrypts and decrypts a 128-bit non-Feistel data block. The number of rounds, such as 128, 192, or 256 bits, is determined by the key size. It consists of 10, 12, or 14 rounds. Every iteration of the AES algorithm will give cloud security. AES employs four transformations: key-adding, mix columns, permutation, and substitution.

4.3. Data Encryption Standard Algorithm

DES is an abbreviation for Data Encryption Standard. The National Institute of Standards and Technology created a symmetric-key encryption technique. The DES structure is a general 16 round feistel structure. DES uses a 64-bit key length. The DES is composed of three major functional structures: the round function, the key schedule, and the final permutation. The avalanche effect and completeness are DES properties. The avalanche effect causes little change in plaintext while producing improved results in ciphertext. Completeness means that every bit has been modified, resulting in a different ciphertext value. The biggest disadvantage of DES is the ease with which data can be hacked.

4.4. AES Algorithm Procedure

Cloud encryption is the process of converting encrypted text from client data. When the data is housed, a potential kind of cloud encryption should be investigated, and it should meet the level of perceptiveness. As more workstations were consumed by encryption, cloud providers only supplied minimal encryption functionality on database fields such as passwords and account numbers. To make the user data exclusive, cloud providers encrypt the whole database of the user or customer before storing it on the server or transferring it via cloud service. When compared to encryption, the processing power of a specific approach is less expensive, and hence such mechanisms are offered by cloud providers in exchange for the encryption process. The most promising technology utilized in encryption mechanisms in today's world is Advanced Encryption Standard (AES), which is one of the most widely used and safe encryption algorithms.

AES algorithm

Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

Initial Round

Add Round Key - each byte of the state is combined with the round key using bitwise
xor

Rounds

SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows - a transposition step where each row of the state is shifted cyclically
a certain number of steps.

MixColumns - a mixing operation which operates on the columns of the state, it combines the four bytes in each column.

Add Round Key

Final Round (no MixColumns)

SubBytes

ShiftRows

AddRound Key

Key generation

Only the first word of the subsection title should be capitalized.

4.5. AES Encryption and Decryption Algorithm

The AES Encryption & Decryption Algorithm follows a step-by-step procedure. The original text is known as plain text, and the encrypted form of data is known as cipher text. The decrypted data will be present in the database as cipher text, but it cannot be read by people or the system without an appropriate mechanism to encrypt it and convert it to readable plain text. The encryption technique differs depending on the changes made in the detailed operation of the algorithm by the keys. The cipher cannot be encrypted or decrypted without the key.

Cipher(byte in[4*Nb], byte out[4*Nb], word
w[Nb*(Nr+1)])
begin

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

They concentrate on AES-256 to make data encryption more efficient in order to protect our sensitive data in cloud computing. The four processing phases of the AES Algorithm are substitute bytes, rows shifted, columns mixer, and round key addition. Along with this, an Advanced Encryption Standard is proposed in order to protect the data confirm of Updating technique is also proposed in this system. This approach provides a tiny and very safe key size, 128-bit keys, in addition to requiring affordable hardware because it executes basic algorithms. The input block and cipher key perform multiple cycle transformations before producing the final output stated in the Rijndeal method, so it is known as an iterative block cipher. This algorithm handles variable-length blocks and variable-key length blocks. The various block length options are 128, 192, and 256 bits long, and each of the nine key combinations is also accessible.

4.6. Proposed VCU Architecture

The initial stage in this process is the verification of anonymised data. The verification of anonymised data is followed by the modification of a table in VCU that allows for data anonymization, verification, validation, and encryption. In order to safeguard the data, the private key is also generated. As a result, only the data owners have access to the data. In the event that attackers are used, data owners will be notified. Figure 4.1 depicts the proposed VCU technique architecture.

Verification: - Verifiable computing allows a computer to offload the computation of a function to another potentially untrustworthy consumer while preserving a verifiable result. When the function's result is returned with the resistance and subsequent users evaluate the function, the estimate will be correctly preceded.

Confirmation: - Confirmation is a method of authentication used to process data or information provided by the provider and the system administrator. It is also a type of allocation and restriction of facilities that the system or the administrator will supply to users.

Updation: - Storage is updated with the database, which is more responsible for keeping data and ensuring that it is accessible. That cloud concern is more secure. It will play a significant role in the realm of data storage. As more and more online purchasing data is transmitted by e-mail and telephone conversation, online shopping continues to thrive. People are drawn to online purchasing, and this industry has evolved. These publicly available social network data lack basic privacy safeguards. It simply substitutes identifying information such as a person's name and data with a meaningless unique identifier. AES parallelization is used in the computer to improve the performance of storage memory.

The main barriers to widespread adoption of public cloud computing are security and privacy. Anonymization is a process that converts original data into garbage for all users except the data owners. This method is utilized in the encryption process. That anonymization process anonymizes the original data into encrypted data, yet it looks exactly like the original data in Figure 4.2. The table depicts user data; it is used to secure the customer's identity. This solution employs the K-anonymity model to safeguard data against individual identification. These table records are similar at least k-1 times, which is ensured when it works with privacy-related attributes. This is usually referred to as a quasi-identifier. This pseudo-identifier is capable of determining the unique identities of any individuals in the general public. Following the current technique, an encryption technique is added to the anonymized data for greater protection. The National Institute of Standards and Technology (NIST) has published this encryption algorithm as a symmetric-key with the cipher block.

4.7. Anonymization with Encryption Architecture

The secure authentication phase of the provided approach is derived by pseudo-code sketching. Initially, the user's code is trusted. This algorithm returns the two solutions. The VCU Secure key first returns the set of user and data verification. After that, it checks the data and feeds it into the K-Anonymity (anonymization) process. After the anonymization procedure is completed, the code is fed into the AES for security reasons AES does not meet the user's requirements. Finally, monitoring update will keep track of user data and code updates. Anonymization is a process that renders original data useless to anyone other than the data's owner.

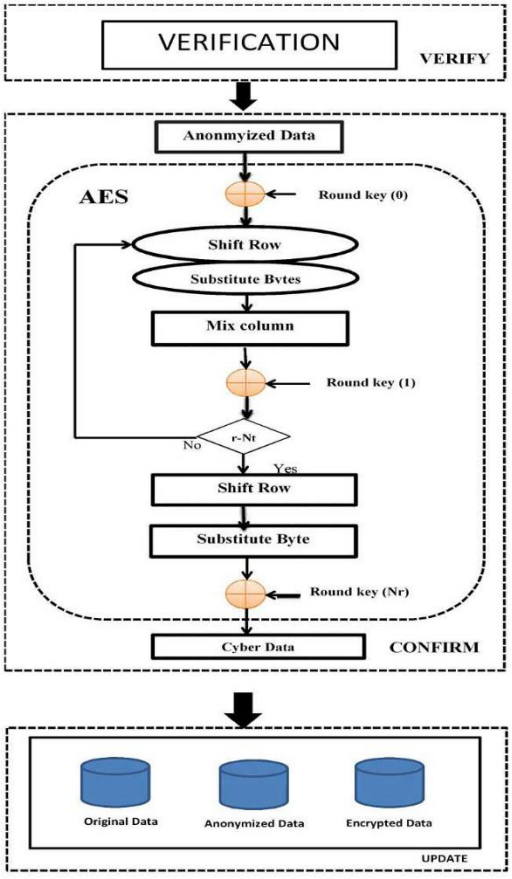

Figure 4.1 Proposed VCU Architecture

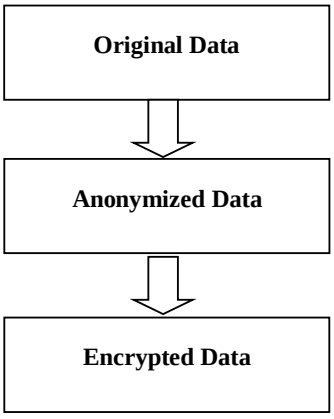

Figure 4.2 Cloud Data Anonymization and Encryption Architecture

The K-anonymity model is employed in this suggested algorithm to shield data from individual identification.

This procedure yields two outcomes. The VCU Secure key first returns a series of user and data verification results. Second, the data is given into the K-Anonymi (anonymization) process once it has been validated by the trustworthy. For security reasons, the code is anonymised before being fed into the AES. The AES does the work that the user specifies. The final stage of the proposed technique is to update all of this data in the cloud service.

That can be denoted as name alvina is anonymized into jadira and the account number 93287463849327 is anonymized into 84196554758418 and the zipcode 75020 anonymized into 7502*. The quasi identifier technique is used for generalization concept. Then anonymized data is moved to further security followed by encryption. Here, this encryption technique makes that anonymized data into the encrypted format by using Advanced Encryption Standard (AES). After that description it moves the data encrypted for more secured process. For example, figure 4 third table the anonymized values for name jadira is encrypted to DqmWZt06QnqqlXYIxwIKzg== and account number 84196554758418 isencrypted to Pkjb693ZXPIe +8SnSeV74lF7Ze3njLV1k7MyHrnpmew= and zip code 7502* is encrypted to 84FCLO051P3GWblAqKEbFA==. From these techniques the data will be secured from hackers or third party. If they decrypt, proposed process encrypts the data also they get only the anonymized data moreover they don't know that the anonymized original information. This process is more secured than the other technique. The below psecdocode sketch is proposed an algorithm for securing authentication that given in algorithm. Initially the user code is trusted.

4.8. Pseudocode of Proposed VCU Method

This method produces two results. VCU Secure key first returns a set of user and data verification. Second, when the data has been verified by the trustworthy, it is fed into the K-Anonymi (anonymization) process. The code is fed into the AES after it has been anonymized for security purposes. The AES performs the work as specified by the user. The suggested algorithm's final stage is to update all of this data in the cloud service.

4.9. Proposed Anonymization and AES Algorithm

TrustedCache ← Data
Trusted Data ← {Update};
TrustedUser ← Φ
While true do D ← Φ;

foreach C € TrustedData do d ← dU
SecrectKey(C);
d←d \ TrustedData;
for each ptr € d do
if K- Anonymi (Code at ptr) then
add code at ptr to AES;
add ptr to TrustedData;
else
accretion non-trusted algorithm;
UpdateMonitor (TrustedData U TrustedUser);
End
The VCU is expansion of Verify, Confirm and Update process.
The algorithm illustrate working module of proposed algorithm.

4.10. Pseudocode Structure VCU with AES Algorithm

Verification

1. Provide the concern secret key (s _key).
2. If (s _key==*matched*), proceeds further.
3. Else authentication failed. Confirmation

For the verified data the code will be changed and encrypted using K-anonymous and AES algorithm respectively.
K _anonymous (data changing):

1. Concern key code will key (s _key)→(c_key)
2. If (s _key), kc : u→ (s _key) and kc: (s_key) → (c _key) a Quasi – identifier of (s _key) will return(c _key).

AES (advanced encryption system):

1. The code encrypted to (c _key) → (c*_key)
2. Thus (c*_key) is the encrypted data for the secret key.

Update
The data will be updated as follows:

1. udate _server1← (s_key)
2. udate _server2← (c_key)
3. udate _server3← (c*key)

End
The provided secret key should be entered, here the key is (s _key) should be checked (s _key==*matched*) then the process will proceed further or else the authentication will fail.
(s _key) → (s _key==*matched*) (1)
The confirmation procedure follows. There are two actions to take under this. The first is k-anonymous, whereas the second is AES (Advanced Encryption System).
K-anonymous (data changing): In this process secret key will be changed. The concern key code (s_key) will be changed to (c _key). If (s _key), kc : u→ (s_key) and kc: (s _key) → (c _key) a Quasi – identifier of (s _key) will return(c_key).
AES (advanced encryption system): The data that is changed using k- anonymous will be encrypted using the AES system.
(c _key) → (c*_key),where (c*_key) (2)
The final process is to update all keys such as the secret key, data change key and the encrypted key are stored in the server udate_server1← (s_key) which is the secret key. udate _ server2← (c_key) is the changed key. udate_server3← (c*key) is the encrypted key of all the data will be stored in the update phase. The equation 1 and 2 give the solution for proposed encryption algorithm.

5. Results and Discussion

Cloud computing is an internet-based technology that connects circulated and similar systems while also providing a virtual system. Three computing resources are provided by the internet cloud computer. The cloud's hardware and software components are handled by a third party on a remote server. It is legal to utilize for both corporations and end users. The dependable services deliver next-generation data centers built on compute and storage virtualization. They are reassured by the most recent cloud computing innovations. The fundamental reason is that users fail to run complex programs and communicate sensitive data over cloud. Trust is commonly used to assess data integrity, reliability, availability, and turnaround efficiency.

5.1. AES with VCU Method Analysis

Cloudsim with 4GB RAM, 2TB hard disk, and Intel i5 processor is employed in this experiment. Cloudsim's simulation experiment is written in Java. It is a cloud computing framework. The simulation is used to create a model of the cloud computing infrastructure and services. Cloudsim offers a variety of

cloud computing service tests. Even after encrypting our personal data, the proposed solution generates a secret key, allowing the customer to relax and begin to trust cloud storage. A data set is a collection of data. The proposed approach compares data set value differences. The data set contains various word files and graphics. Each data set has a distinct size.

Verification time: - Data will be entered here and checked for authenticity. Take, for example, file set 1, where the DES-VCU approach takes 729ms to complete the verification procedure but the AES-VCU method only takes 643ms.

Consider file set 2, where the DES-VCU method takes 742ms and the AES-VCU approach takes 689ms. As a result, the verification time is quick as compared to the previous system. The proposed technique yielded the best results, as illustrated intable 5.1 and Figure 5.1.

Table 5.1Verification Time Comparison

Data set	DES-VCU (Millisecond)	AES – VCU (Millisecond)
File Set 1	729	643
File Set 2	742	689
File Set 3	713	613
File Set 4	703	620
File Set 5	781	603

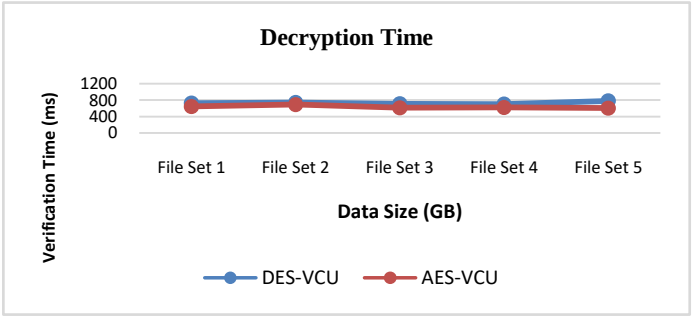

Figure 5.1 Verification Time Analysis

Execution time for Client: - After the client's verification and encryption, data will be entered here and processed for execution. Consider entering 2 GB of data, which will be executed in 832ms using the DES-VCU method, but the same data amount using the AES-VCU method will take just 801ms. Similar technique 3GB data should be submitted in encryption process, DES-VCU method 921ms, but similar data size 937ms encryption process time. Encryption time varies depending on data amount and method. The proposed methodology's overall and average encryption procedure takes less time for client-side encryption. The suggested solution reduces encryption time complexity in the server, as illustrated in Figure 5.2 and Table 5.2.

Table 5.2 Client-Side Execution Time Comparison

File size	DES-VCU (Millisecond)	AES – VCU (Millisecond)
1GB	402	432
2GB	832	801
3GB	921	937
4GB	1042	1002
5GB	1263	1260

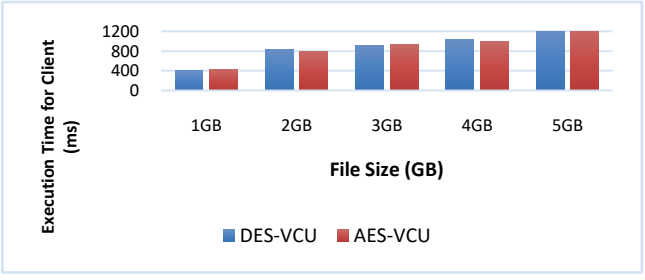

Figure 5.2Client-side Execution Time Analysis

Execution time for Server: - Data should be entered here; it will be processed for execution after the server's verification and encryption process. Consider entering 2GB of data, which will be executed in 1606ms using the DES-VCU method, but the same data amount using the AES-VCU method will only take 1593ms.

Methods that are similar When 1GB of data is entered into the encryption process, the DES-VCU approach takes 792ms, but equivalent data takes 837ms. Encryption time should be changed depending on data amount and method. The proposed methodology for overall and average encryption takes less time for server-side encryption. The suggested solution reduces encryption time complexity in the server, as illustrated in Figure 5.3 and Table 5.3.

Table 5.3 Server-Side Execution Time Comparison

File size	DES-VCU (Millisecond)	AES – VCU (Millisecond)
1GB	792	837
2GB	1606	1593
3GB	1812	1847
4GB	2051	1978
5GB	2429	2412

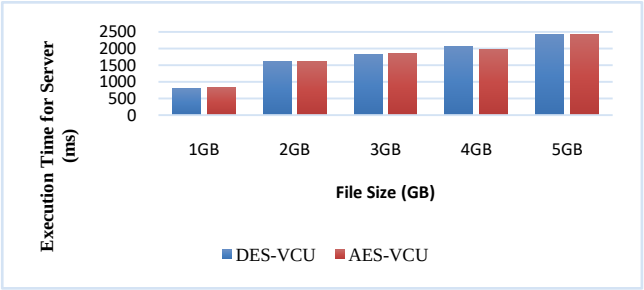

Figure 5.3 Server-side Execution Time Analysis

CPU Utilization Time Analysis: - CPU usage refers to the computer system's greatest percentage level consumption during algorithm execution. For the input procedure, many sizes of data sets are used. The file set 1 is sent to the full process, which will consume 60% of the time in the DES-VCU approach. The identical data set AES-VCU technique consumes 58% of the CPU. The proposed approach in file set 3 consumes 61% of the CPU. The present approach for the same data set takes 62%. In compared to existing systems, the suggested solution requires less CPU consumption, with both methods occasionally achieving near-identical utilization levels. The primary finding of this study is that the proposed strategy has no effect on system performance. The CPU utilization indicates the QoS parameter indirectly. Variation of less than 5% has no effect on performance. The CPU Utilization and Performance Analysis are depicted in Figure 5.4 and Table 5.4.

Table5.4 CPU Utilization Comparison

Algorithm	File Set 1	File Set 2	File Set 3	File Set 4	File Set 5
AES-VCU	58%	50%	61%	43%	85%
DES-VCU	60%	49%	62%	41%	84%

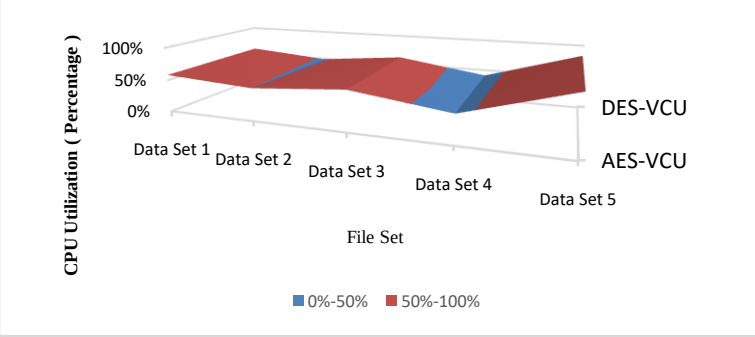

Figure 5.4CPU Utilization Analysis

Execution Time Analysis: - The execution time analysis is explained in table 5.6. The encryption and deduplication processes can be used to calculate the execution time analysis. Consider data set 1, which took 0.4527 seconds to complete without the deduplication process. With the deduplication procedure, it takes 0.4912 seconds. In data set 2, the execution time is 0.4786 seconds without the deduplication method, and it is 0.7281 seconds with the deduplication method. Consider data set 4, where the execution time without the deduplication process is 0.7364 seconds and the execution time with the deduplication process is 0.8833 seconds. Consider data set 5: without deduplication, it takes 0.332 seconds to complete, while with deduplication, it takes 0.5423 seconds. This demonstrates that the execution time grows during the deduplication process since repeated data may be repaired rapidly, but massive amounts of data cannot be fixed quickly.

Table 5.6 Execution Time Comparison

Execution Method	File Set 1	File Set 2	File Set 3	File Set 4	File Set 5
Without DD(Sec)	0.4527	0.4786	0.6754	0.7364	0.332
With DD (Sec)	0.4912	0.7281	0.9463	0.8833	0.5423

6. Conclusion

The proposed method's goal is to save storage space while improving cloud security. The module's initial phase is to combine the anonymization approach and the AES algorithm. The proposed solution is to use the AES algorithm to introduce the VCU method. VCU is an acronym that stands for Verify, Confirm, and Update. The authorized process is utilized for verification and confirmation, and it is then updated in the cloud server. For the encryption process, the Advanced encryption method is applied. The average execution time of the DES-VCU method on the client side is 4460 milliseconds. The AES-VCU technique has a client-side average execution time of 4432 milliseconds. The present and proposed methods differ by 28 milliseconds. The CPU utilization of the existing DES-VCU approach is 59.2%, while the CPU utilization of the suggested AES-VCU method is 59.4%. The only difference is a 0.2% increase in CPU use.

Security will be offered as a service to users based on their requirements. The user can make the decision based on the pricing. They must pay for the security in exchange for the value of the assets under consideration. This framework enables a regular user who does not require security to use the same cloud as high-value assets. In actuality, the average user does not have to pay anything for security, but high-value assets must make a trade-off and set aside a significant sum of money to enable security.

Quality and profit are always required by the industry for their services. The increase in security is to fulfill the quality factor.

7. FutureWork

In addition to the existing modules, a separate framework for data security is being transmitted with third-party services. It will increase the reliability and trustworthiness of the cloud environment. Such a mix of security modules will foster user trust and encourage people to keep data in the cloud and take use of its benefits without sacrificing security.

The hybrid algorithm will only test a specific data range. Because of its booming technology, the same principle can be utilized in larger data sets in the future; they are confronting a lot of security challenges in this big data arena.

REFERENCES

[1] Abadi, M, Boneh, D, Mironov, I, Raghunathan, A &Segev, G, 'Message-Locked Encryption for Lock-Dependent Messages'. In Advances in Cryptology (CRYPTO 2013), International Conference of the Springer, Lecture Notes in Computer Science, vol. 8042, pp. 374- 391, 2013.

[2] Bellare, M, Keelveedhi, S &Ristenpart, T, 'Message-Locked Encryption and Secure Deduplication'. In Theory and Applications of Cryptographic Techniques, International Conference of the Springer, Lecture Notes in Computer Science, vol. 7881, pp. 296-312, 2013.

[3] Che, J, Duan, Y, Zhang, T & Fan, J, 'Study on the security models and strategies of cloud computing'. In Power Electronics and Engineering Application, International Conference of the Procedia Engineering Elsevier, pp. 586-593, 2011.

[4] Chen, Y & Sion, R, 'On Securing Untrusted Clouds with Cryptography'. In Privacy in the Electronic Society, 9th Annual Workshop of the WCE, pp. 109-114, 2012.

[5] Junaid Hassan, Danish Shehzad, Usman Habib, Muhammad Umar Aftab, Muhammad Ahmad ,RamilKuleev , and Manuel Mazzara, ' The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR)' , Computational Intelligence and Neuroscience, Hindawi, Volume 22, June 2022, pp. 1-26, 2022. https://doi.org/10.1155/2022/8303504

[6] Kouatli, I, 'Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management'. In Information Technology and Quantitative Management (ITQM 2016), International Conference of the Elsevier, Procedia Computer Science, vol. 91, pp. 412-421, 2016.

[7] Lee, K, 'Security threats in cloud computing environments'. International Journal of Security and Its Applications, vol. 6, no. 4, pp. 25-32, 2012.

[8] Liu, Z, Chen, X, Yang, J, Jia, C & You, I, 'New order preserving encryption model for outsourced databases in cloud environments'. Journal of Network and Computer Applications, vol. 59, no. 1, pp. 198-207, 2016.

[9] Mahajan, P & Sachdeva, A, 'A Study of Encryption Algorithms AES, DES and RSA for Security'. Global Journal of Computer Science and Technology, vol. 13, no. 15, pp. 01-07, 2013.

[10] Mansukhani, B & Zia, TA, 'An empirical study of challenges in managing the security in cloud Computing'. In Information Security Management, 9th Australian International Conference of the Research Online, pp. 172-181, 2011.

[11] Manzoor, A, 'Cloud Computing Applications in the Public Sector'. Cloud Computing Technologies for Connected Government, pp. 215-245, 2016.

[12] Meetei, MZ & Goel, A, 'Security issues in Cloud Computing'. In Biomedical Engineering and Informatics (BMEI), 5th International Conference of the IEEE, pp. 1321-1325, 2012.

[13] Munir, K &Palaniappan, S, 'Secure cloud architecture. Advanced Computing'. Advanced Computing: An International Journal (ACIJ), vol. 4, no. 1, pp. 09-22, 2013.

[14] Paul, M & Mandal, JK, 'A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept'. In Information Technology, Electronics and Communications (ICITEC–2013), International Conference of the IAIRS, pp. 06-11, 2013.

[15] Rohit, B &Sanyal, S, 'Survey on security issues in cloud computing and associated mitigation techniques'. International Journal of computer applications, vol. 47, no. 18, pp. 0975-0888, 2012.

[16] Sachdev, A & Bhansali, M, 'Enhancing cloud computing security using AES algorithm'. International Journal of Computer Applications, vol. 67, no. 9, pp. 1-6, 2013.

[17] Sharma, S, Verma, A, Singh, S & Pandey, V, 'Data Protection in the Cloud: Dynamic Password Authentication and Certificate-Based Authorization'. In Cloud,Big Data and Trust, International Conference of the Cloud, pp. 13-15, 2013.

[18] Singh, J, Krishnan, L & Anil Kumar, S, 'An Overview of Cloud Computing with Security Issues'. Journal of Computer Science and Applications, vol. 4, no. 1, pp. 1-7, 2012.

[19] Sood, SK, 'A combined approach to ensure data security in cloud computing'. Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838, 2012.

[20] Sudha, M & Monica, M, 'Enhanced security framework to ensure data security in cloud computing using cryptography'. Advances in Computer Science and its Applications, vol. 1, no. 1, pp. 32-37, 2012.

[21] Sujaritha , Akshara D , Ashfak Ahamed A , Chandhinishri V S, 'Privacy Preserving Verification Scheme for Cloud Platform Using DML' ICCCEBS 2021, Journal of Physics: Conference Series, pp. 1-5, 2021. doi:10.1088/1742-6596/1916/1/012154.

[22] Tebaa, M, El Hajji, S & El Ghazi, A, 'Homomorphic Encryption Applied to the Cloud Computing Security'. In World Congress on Engineering (WCE), International Proceedings of the WCE, vol. 1, pp. 4-6, 2012.

[23] Ubale, SA, Apte, SS &Bokefode, JD, 'Developing Secure Cloud Storage System Using Access Control Models'. In Data Engineering and Communication Technology, Springer International Conference of Advances in Intelligent Systems and Computing, vol. 469, pp. 141- 147, 2017.

[24] Vijay, GR, & Reddy, ARM, 'An Efficient Security Model in Cloud Computing based on Soft computing Techniques'. International Journal of Computer Applications, vol. 60, no. 14, pp. 12-16, 2012.