Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Ameliorate Data Security in Cloud Using Hybrid Cryptography and Key Management Proficiency

Dr. R. Kaviarasan, Cheviti Jahnavi, Saddala Akhila Reddy, Panditi Swetha, G. M. Venkateswar Reddy

Department of CSE RGMCET, Nandyal, India
Email: Kaviarasanr64@ptuniv.edu.in

As cloud computing has revolutionized data storage and control, ensuring facts security in cloud environments has turn out to be a vital concern for groups and individuals alike. Encryption strategies, each at rest and in transit, arc crucial for protecting statistics from unauthorized access and breaches. The abstract also addresses rising threats and fine practices for enhancing cloud security, emphasizing the want for a multi-layered protection technique and non-stop tracking. As cloud adoption grows, strong statistics security measures remain vital to shield sensitive statistics and maintain user trust. The suggested device uses hybrid cryptography, a well-liked strategy that combines the advantages of symmetric and asymmetric cryptography to achieve exceptionally high levels of performance and security.We also recommend a key management system that includes producing and storing the symmetric keys at the patron aspect, in preference to at the cloud server. This ensures that the keys continue to be under the manipulate of the consumer, in preference to the cloud issuer, and reduces the chance of key robbery or leakage. Experimental evaluation demonstrates the efficacy of the proposed approach in enhancing facts safety in cloud environments. The consequences indicates reduction in encryption processing time, discount in key change time, boom in information switch safety, lower in computational overhead, development in ordinary machine overall performance in comparison to traditional encryption methods.

Keywords: Cryptography, symmetric and asymmetric cryptography, key management system, Security, multi-layered security.

1. Introduction

These days,organizations and individuals are moving to the cloud because it is more convenient and less expensive.A recent development in computer science is cloud computing.In order to describe it, Mell and Grance (2011) used (p. 1). According to this definition, "Cloud computing is a version for allowing ubiquitous, convenient, on-call network access to a shared pool of configurable computing assets (e.g. networks, servers, garage, applications, and offerings) that may be unexpectedly provisioned and launched with minimal management effort or service provider interaction." “Cryptograph became derived From Greek phrases kryptos (krnptos), which means hidden or mystery, praphia (graphia) meaning writing.The study of methods to ensure the confidentiality and/or validity of statistics is known as cryptographic algorithms (Stalling, 2014). Symmetric key encoding, also known as mystery key encryption, uses only one secret to encrypt and decrypt statistics while using public and private keys in an uneven fashion. The public key is used for encryption, while the personal secret is utilized for decryption (Elminaam et al., 2010). Triple statistics, DES, and AES Symmetric methods include the encryption set of rules (3DES), Rivest Cipher 4 (RC4), and Blowfish (Chandra et al., 2015). Elliptic curve schemes, the virtual Signature set of rules (DSA), and EIGamal, Rivest, Shamir, and Adelman (RSA) are examples of asymmetric techniques at the same time.It has been noted that in order to support the increased security in cloud storage, a strong authentication scheme must be developed. The majority of the reviewed studies overlook consumer authentication, and the majority of research ignores the three requirements of information security authentication,confidentiality, and integrity which leaves gaps for attackers.The primary goal of this study is to design and implement a secure and environmentally friendly hybrid cryptographic set of rules for cloud data security.

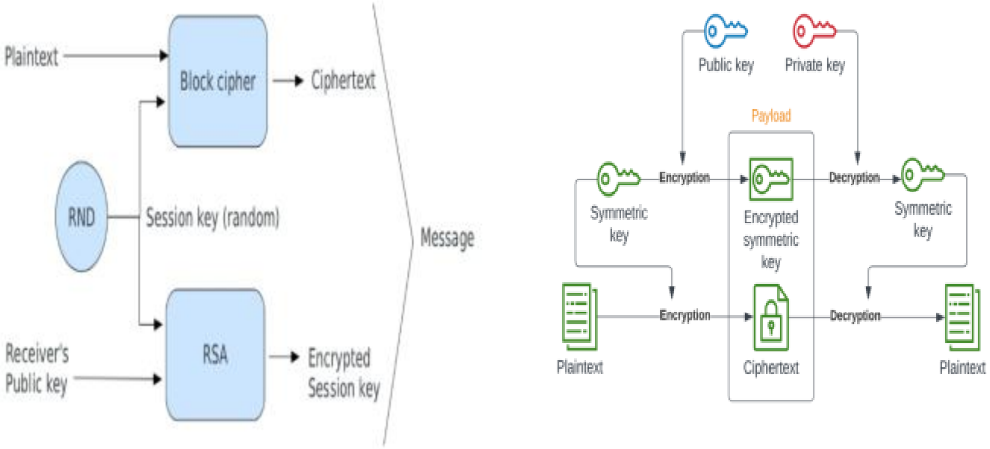


Fig.1. Architecture of encryption and decryption process

This hybrid encryption technique uses a dynamically generated key for information encryption and decryption in order to provide secrecy, integrity, and authenticity. Using the created keys, the facts are encrypted and decrypted using three symmetric algorithms: DES, AES, and Blowfish. Every day, more and more data will be transferred from cellular devices to the cloud. Due to its accessibility, usability, and above all the ability to link cellular and cloud computing, cellular cloud computing has become a crucial field in recent years. Through a community, cloud facts are transferred from a cell to the cloud and vice versa, which is crucial for securely switching records. An encryption set of rules may be necessary in the modern era to secure sent statistics with high overall performance in a short amount of time.The suggested device's purpose is to provide an encryption system that can efficiently encrypt and decrypt reports containing information sent from mobile devices to the cloud. In addition to providing a collection of encryption algorithms that aid in record encryption, this work demonstrates a system for encrypting cellular-cloud statistics. The device will help cell-cloud users improve the security of their transmitted and received data and prevent it from being stolen.

2. Literature Survey

On this phase, a study of various current techniques is presented, together with the benefits and barriers of these strategies.

Rohini et al., (2018) Proposed hybrid RSA method for cloud computing. The research centered on protection issues on cloud. They use a set of cryptographic rules to safely encrypt the data via the cloud. Additionally, they use hash codes to preserve the integrity of the data. In their study work, Richa et al. (2017) suggested a hybrid set of guidelines that combines AES protection techniques with MD5 hash to ensure clients' data security in the cloud.In the current situation, the hybrid method virtually guarantees statistics security.The set of rules' main premise is that using a weak encryption for each encryption and deciphering could make it extremely vulnerable to malevolent attacks. Therefore, this problem is fixed in the suggested approach by employing sophisticated encryption techniques for both encryption and decryption. Before gaining access to the particular cloud provider, the user who needs to access the information must submit the login ID, password, OTP (one-time password), and CAPTCHA that were delivered to the registered cell phone.

Taha et al. (2017) acknowledged that the amount of information being sent over the internet is growing daily. It has become necessary to have a set of encryption standards that ensure records are transmitted securely and swiftly. A version for encrypting sent cloud statistics was suggested by the authors. This approach creates a novel encryption method that encrypts and decrypts transmitted data by utilizing the encryption algorithms RSA, Triple DES, RC4, and Krishna.

Timothy et al., (2017) presented a novel method for cloud information security by utilizing a hybrid cryptosystem. The goal of current research is to encrypt customer data in order to protect statistics from hackers or unwanted access during information transmission. This hybrid cryptosystem is made up of both symmetric and uneven cryptography techniques. The RSA uneven algorithm handles authentication, while the Blowfish symmetric algorithm handles fact confidentiality. For data integrity, this method also incorporates the comfortable hash algorithm-2 (SHA-2).

Biswas et al., (2019)reported that steganography improves security and hybrid cryptography offers greater security. The authors put out the concept that utilizes both AES and RSA in order to accomplish hybrid cryptography. AES is used to encrypt the message. The security level is raised by using the RSA public key to encrypt the symmetric key used for message encryption. Using the RSA public key to provide a virtual signature, a hash cost of the message is computed once it has been encrypted again. This virtual signature aids in verifying the message's integrity on the receiving end. These encrypted files—that is, the encrypted digest, the encrypted message, and the encrypted key—have been joined to create a single message. This entire message has been encrypted using the LSB (Least Sizeable Bit) steganography technique. According to the writers, the suggested device's resistance to attack has been guaranteed. Consequently, this collection of guidelines offers confidentiality, integrity, and authentication all at once.

Paranjothi et al.,(2018) gave an overview of cloud computing for cellular devices. Additionally, they presented the cell cloud computing discussion framework, which focuses on offloading, privacy, and wireless distributed computing. At one point in the literature review, they concluded that cell cloud computing is a technologically valued and appropriate type of virtual communication in terms of digital devices that store data in the cloud and a distributed environment. They also categorized the disadvantages of cellular cloud computing in terms of privacy.

Lakshmi et al., (2017) provided an anonymous privacy protection technology called "Slicer" is used to detect multimedia data files stored on cloud computing. It combines message transfer strategies with information coding techniques. to ensure that user records are comfortably protected while also upholding privacy and confidentiality.value transfer decreased and switched These information-switching techniques are used during meetings. Two concurrent algorithms—the approximation method and the heuristic algorithm—were employed to achieve the least amount of charge transfer. excellent provision of fundamental information with minimal verbal interaction.

Barhoom et al., (2018) proposeda way to reduce the burden of privacy while conserving and reducing processing, memory, and power. This is accomplished by encrypting data in mobile cloud computing using a symmetric set of rules, sending it to the personal cloud, and then encrypting it once more before sending it to the public cloud using an uneven algorithm. The following experimental findings were validated following a comparison of encryption techniques that required significantly less time and decryption time: For symmetric, use the Blowfish algorithm; for asymmetric, use the DSA set of rules. The results of the investigation demonstrated a remarkable improvement in reducing the sources within the time frame and energy consumption and processor.

Debabrata et al.,(2019) methodically investigated the privacy and security issues and introduced a version based mostly on cryptography to manage several requests from a few devices for MCC. Through the use of encryption, decryption, and message digests, their approach makes it easier to authenticate vocal communications between clients and service providers.

Gill et al., (2019) provided a comprehensive overview of the several green frameworks that are available for offloading computing from the cell to the cloud environment. Strength saving,the most important criterion of SMDs,is the primary objective of all these frameworks.Offloading the electricity intensive components of mobile packages to the cloud environment may help overcome the limitations of SMDs, such as their poor execution speed, low computing power, and shorter battery life. The frameworks are grouped according to the offloading option (static or dynamic), the center factor that facilitates offloading, the different parameters that may be examined before or during offloading, and the many real-world packages that can be used with those frameworks.

Patil et al., (2018) introduced a minor cloud-based garage system. For attribute-based whole document querying, this framework offered an easy-to-use document navigation service. In addition, it has a useful form that allows users to check the accuracy of their statistics, which could reduce the strain on mobile devices. The suggested framework is strong enough to offer flexible records sharing in cellular computing environments,according to experimental simulations.

Alotaibi et al., (2019) examined the elements that influence the decision to use SaaS. The study depends on developing a revised version that is mostly centered at the UTAUT. By making QoS the primary antecedent of BI, consistent with its role in online offerings, the proposed model provides a comprehensive explanation for the adoption behavior of software as an offering. However, in order to accommodate the uptake of SaaS in developing countries, education was incorporated into the model as a moderating factor.The version was changed to examine empirical data gathered through the use of questionnaires. Using the encryption time, memory output byte usage, and battery power, researchers found in the literature assessed a related analysis of encryption algorithms such as DES, AES, Blowfish, RC2, 3DES, and RC6 for information transfer. The performance of selected symmetric key algorithms was also examined in the study. Safety risks, significant frequent attacks, and numerous safety measures that protect customers from attacks and incursions were all analyzed by builders. It develops a new set of hybrid cryptography rules and analyzes them using unique hybrid cryptography algorithms based on throughput, encryption time, and power consumption.

Table 1: Summary Table of Literature Survey

S. No.	Authors	Methodology	Advantages	Disadvantages
1.	Rohini et al., (2018)	Hybrid RSA with HMAC integration.	Enhanced data Security,Data Integrity Maintenance	Increased Computational Overhead,Complexity in Key Management
2.	Taha et al. (2017)	Combines RSA, Triple DES, RC4	Enhanced Security,Flexibility	Complexity and Key management
3.	Timothy et al., (2017)	Blowfish, RSA, SHA-2 hybrid system.	Data confidentiality, Authentication, Integrity	Complex Implementation,Key Management,Performance Overhead
4.	Biswas et al., (2019)	AES, RSA, hash, LSB steganography	Confidentiality,Integrity, Enhanced security	Steganography limitations,Processing Overhead
5.	Barhoom et al., (2018)	Blowfish, DSA, symmetric, asymmetric encryption	Privacy,Time reduction, Resource efficiency	Complexity,Integration Challenges,Scalability Issues
6.	Gill et al., (2019)	Energy-efficient frameworks,mobile cloud offloading	Offloading flexibility,Energy Saving	Network Dependency,Complexity
7.	Alotaibi et al., (2019)	UTAUT model,SaaS Adoption	Power Efficiency,Encryption Optimization	Data dependency, Model Assumptions

The Hybrid Cryptography approach, which merges AES and RSA, is better at key management and encryption performance compared to the methods used by Biswas et al. (2019) and Patil et al. (2020). In the AES and RSA model, AES is faster in encryption and decryption because it is symmetric, whereas RSA is slower but is used only for encrypting the AES key, making the overall encryption performance efficient. This model exhibits excellent skills in key management as RSA successfully allows the safe transmission of the AES key and hence establishes a systematic and safe means of key exchange. In contrast, Biswas et al. (2019) utilize a combination of AES, RSA, and SHA-2 along with steganography to enhance security, though increased complexity and overhead due to steganography might slow down the performance. The methodology presented by Patil et al. (2020) emphasizes data integrity and flexible cloud-based sharing but lacks a well-defined structured approach towards encryption and key management. Even though both the papers discuss benefits in terms of security, especially integrity verification and data sharing, the hybrid AES-RSA cryptography model provides better overall performance with respect to encryption and decryption efficiency with increased security benefits, due to optimized implementation of both symmetric and asymmetric methodologies of encryption.

3. Proposed System

This study proposes a hybrid set of rules to decorate protection of cloud data the usage of encryption set of rules.The primary goal of using encryption methods is to store or make large volumes of data more comfortable. If the safety issues are fixed, it can be said that cloud garages will be the solution of the future for both small and large businesses.Building an encryption device that can successfully encrypt and decrypt documents while transferring data from cellular to cloud is the goal of the suggested machine. with addition to offering a collection of encryption algorithms that aid with fact encryption, this study proposes a device for encrypting cell-cloud data. The device will assist cellular-cloud users in strengthening the security of their transmitted and acquired data and preventing its theft.While RSA securely encrypts and exchanges the AES key, AES is utilized for green encryption of large statistics. As a result, there is no longer a need for direct dissemination of the data that is transferred from cellular devices to the modern cloud, which is growing daily. These days, mobile cloud computing is crucial because it is readily available, easy to use, and—most importantly—connects mobile devices to cloud computing. Through a network, cloud records are sent from cellular devices to the most recent cloud and vice versa, which keeps us informed and, crucially, allows us to transfer data securely. These days, an encryption set of rules may be essential for safeguarding data transmissions with good overall performance in the shortest amount of time.

4. Methodology

For even more remarkable results, this novel hybrid cryptography technique combines all symmetric and asymmetric sets of principles.The encryption and decryption machine is followed by every cryptographic approach. The exact facts are transformed into current cipher records using an encryption technology that no human or individual can decipher. The decryption method is used to obtain the specific statistics from the cipher statistics. The symmetric and uneven set of rules used in this examine-time encryption and decryption system is up to date.

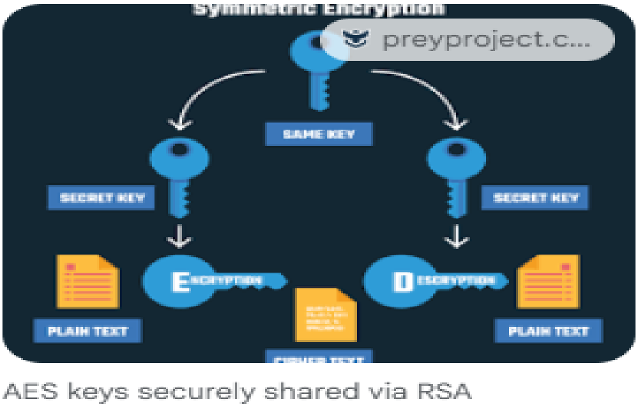


Fig.2. AES keys securely shared via RSA

Securely Sharing AES Keys through RSA: A

Hybrid technique:

Symmetric Encryption (AES): rapid and efficient for bulk facts encryption, however requires a at ease method to share the secret key.

Asymmetric Encryption (RSA): Slower however lets in at ease key change with out pre-sharing a secret.

The Hybrid solution:

Generate AES Key:A random AES secret's generated.

RSA Encryption: The recipient's public RSA key is used to encrypt the AES key.

Transmission:The recipient receives the encrypted AES secret safely.

RSA Decryption: The AES key is decrypted by the recipient using their private RSA key.

Records Encryption/Decryption:Records can now be encrypted and decrypted using the shared AES key between the sender and the recipient.

Securely Sharing AES Keys through RSA: A Hybrid approach

Symmetric Encryption (AES): speedy and green for bulk information encryption, however calls for a at ease technique to proportion the name of the game key.

Uneven Encryption (RSA): Slower but permits comfortable key alternate with out pre-sharing a secret.

The Hybrid solution:

Generate AES Key: A random AES key's generated.

RSA Encryption: The recipient's public RSA key is used to encrypt the AES secret.

Transmission: The encrypted AES key's securely transmitted to the recipient.

RSA Decryption: The recipient decrypts the AES key using their private RSA key.

Statistics Encryption/Decryption: The recipient and sender can now use the shared AES key to encrypt and decrypt data.

Key factors:

Protection: RSA encryption ensures that handiest the intended recipient can decrypt the AES key.

Performance: AES is used for efficient encryption of the actual facts.

Key management: RSA simplifies key management by means of eliminating the need for direct distribution of symmetric keys.

Additional considerations: Key Lengths: select appropriate key lengths for both AES and RSA based on safety necessities.

Key garage: Securely shop RSA personal keys to save you unauthorized access.

Implementation: bear in mind the usage of established cryptographic libraries for relaxed and efficient implementation.

Actual-global applications:

At ease communication: HTTPS, SSL/TLS protocols use this method for at ease net surfing.

Report Encryption: gear like GPG and PGP frequently rent this approach for encrypting files.

Cloud storage: Cloud carriers may also use this to encrypt user facts at relaxation.

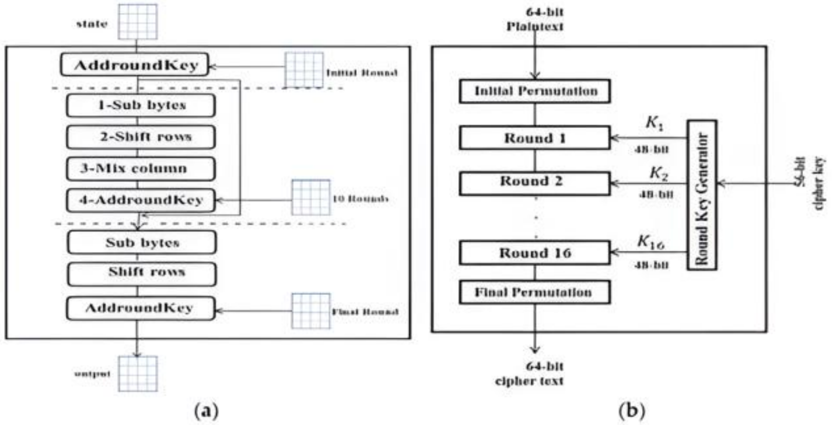
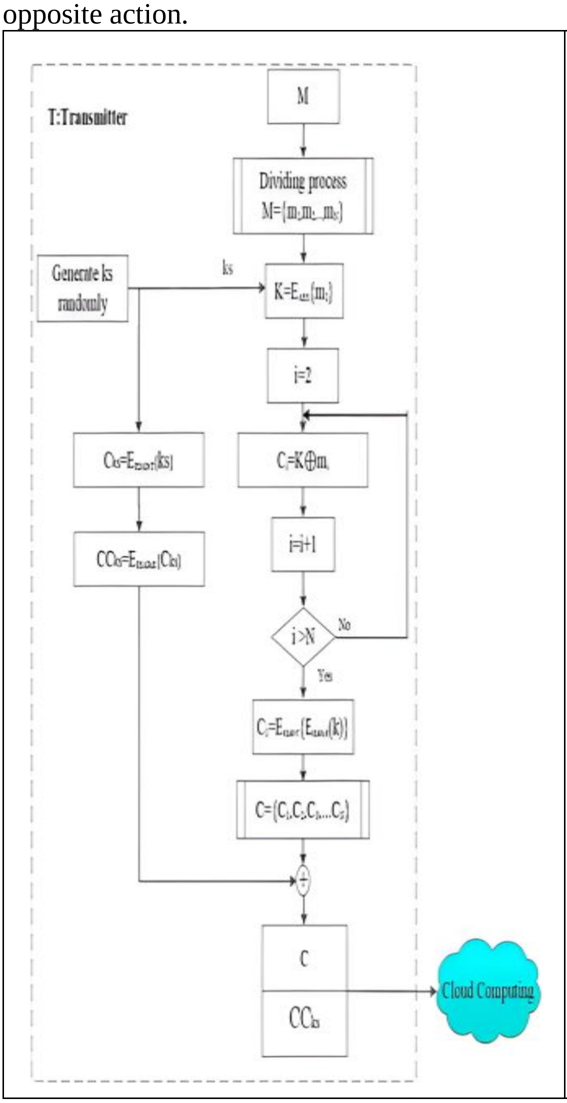


Fig.3. Multi-Tenant Environment 64bit encryption and decryption process

The proposed hybrid model that combines the RSA and AES algorithms:

Below figure demonstrates The hybrid suggested approach, which combines the RSA and AES algorithms on the transmitter's end, aims to meet cloud computing security needs while achieving excellent confidentiality and the shortest execution time. Divide the plain text M into (N) blocks of length 128 bits, and then encrypt the message blocks {m2, m3, ……, mN} according to the key (K). The key (K) is the outcome of ciphering the first block (m1) using the AES algorithm with a dynamic key (KS), which is generated at random each time. This key (KS) is then protected with two stages of encryption using the RSA algorithm. This is the basic idea behind the proposed model,first with the transmitter's private key (ERSAPrT) and then with the receiver's public key ((CK) ERSAPuR). Then, using the same mechanism of protection as the dynamic key (KS), the key (K) is used to encrypt the mi blocks where (i = 2, 3,…., N). The encrypted text (C) is then combined with the encrypted key (CCKS), which has already undergone two levels of encryption. Whether the procedure is storing or communicating, the message is then transmitted to the cloud, and the recipient performs the opposite action.



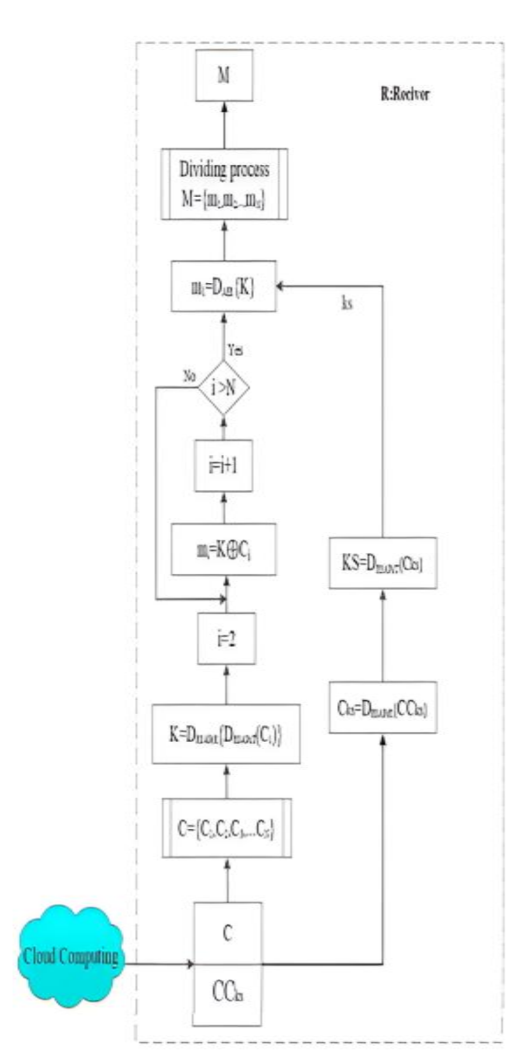


Fig.4. The hybrid model transmitted side Fig.5. The hybrid model receiver side

RSA and AES

Comfortable up to date updated manage is enforced by means of Key management systems

(KMS) up-to-date ensure proper tenant isolation.

Hybrid Algorithm:

```
from cryptography.hazmat.primitives.asymmetric inport  rsa
from cryptography hazmat. primitives. asymmetric. padding import RSAES OAEP
from cryptography hazmat. primitives import hashes
from cryptography .hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography .hazmat.backends import default_backend
# Generate ASA key pair
private_key = rsa.generate_private_key(
public_exponent=65537,
key_size=2048,
backend=default_backend()
)
public_key = private_key. public _key()
# Generate AES key
aes_key = os.urandom(32) # 256-bit AES key
# Encrypt AES key with RSA public key
encryptor = Cipher(
algorithms.RSAES OAEP(mgf=NGF1(algorithm=hashes.SHA256()),
algorithm=rashes,SHA256(), label=None) ,
backend=default_backend() ,
).encryptor()
encrypted_aes key = encryptor.update(aes_key) + encryptor.finalize()
# Transmit encrypted aes key to recipient
# Recipient decrypts AES key with RSA private key
decryptor = Cipher(
algorithms.RSAES OAEP(mgf="GF1(algorithm-hashes.SHA256()),
algorithm=rashes.SHA256(), label=None) ,
backend=default_backend() ,
).decryptor()
decrypted_aes_key = decryptor.update(encrypted_aes_key) + decryptor. finalize()
```

Both sender and recipient can now use the shared AES key for data encryption/decryption|

Hybrid algorithm Encryption precept: The hybrid encryption algorithm employs two-layer AES and RSA encryption, and the encryption manner goes via a series of modifications and steps. The moves involved in the two strategies' report encryption schemes are specified underneath within the order of encryption. The AES set of rules clusters the processing units, and the ordered 128-bit information is assigned to a four-by means of-4 nation matrix. All ameliorations within the algorithm are completed and targeted at the country matrix. Four truthful mathematics operations—Sub Bytes, Shift Rows, mix Columns, and add round Key are used within the technique.

Hybrid set of rules Decryption principle: within the hybrid set of rules, the personal key of the RSA set of rules is used to decode the cipher text encrypted by using the general public RSA key in the first layer, after which the AES secret is used to decrypt the cipher textual content and get the plaintext. As RSA decryption is used, the encrypted cipher textual content c is decrypted and transformed, and the simple textual content m is acquired through the following calculation.

m = cd mod n

here, d is calculated with the aid of the important thing era algorithm, and n is the manufactured from the massive high numbers p and q within the decryption method of the AES algorithm, Sub

Bytes, Shift Rows, and mix-Columns are the inverse operations of the encryption procedure. nonetheless, in upload spherical Key, the inverse operation is similar to the forward transformation due to the fact the X-OR operation is its very own inverse

Select legit Cloud service companies:

Whilst choosing a cloud provider, opt for reliable vendors with a tune report of robust security features. search for enterprise leaders who prioritize encryption, facts redundancy, and compliance with industry standards. UT uses Microsoft One Drive for secure on-line storage. non-public cloud services up to date never be used updated shop college information.

Study Passwords and Multi-updated

Authentication (MFA):

A sturdy password is your first line of defense. make certain it's miles complex, unique, and now not without difficulty guessable. imposing Multi-thing Authentication provides an extra layer of protection by using requiring a 2nd form of verification, up-to-date a one-time code despatched on your cell up to date. most private cloud vendors offer some type of multi-updated authentication up-to-date keep your private data cozy.

1. Statistics Encryption:

Encryption scrambles your facts right into a code that's almost impossible up to date decipher without the right key. ensure that your cloud provider makes use of strong encryption protocols, each in transit (at some point of transfer) and at rest (while up-to-date).

2.Records classification and up to date control:

Categorize your facts based on updated on its sensitivity. Limit up to date up to date sensitive updated data handiest up-to-date legal employees. frequently assessment and update permissions up to date prevent unauthorized up-to-date.

3. Everyday Backups:

Usually preserve backups of your crucial facts. Cloud companies frequently offer computerized backup answers that can be helpful in case of facts loss or cyber incidents.

4. Stay knowledgeable and educated:

live modern with the present day trends and excellent practices in cloud security. Attend workshops, webinars, or education classes from relied on enterprise assets.

5. Up-to-date for Suspicious activity:

Regularly up to date display your cloud money owed for any uncommon or unauthorized up-to-date. Many cloud providers offer up-to-date and notifications up-to-date warn you updated suspicious activities

6. Compliance and guidelines:

Be aware of updated any enterprise-particular compliance necessities or regulations that follow updated the university and comfy your information thus. a few examples of up-to-date data encompass HIPAA, PCI, and GLBA.

7. Incident response Plan:

Have a clean plan in area up to date respond updated capability safety incidents, which includes steps for reporting, investigating, and mitigating any breaches. Your first step updated reporting a

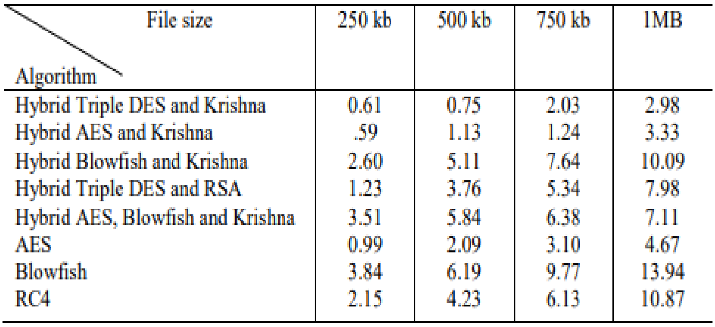
suspected incident is up to date touch the OIT Helpdesk.

7.1. Throughput: The proposed system examines throughput and the encryption time for a collection of algorithms used for encryption to encrypt data transmitted from cell to cloud. more than one amalgamation changed into designed to put in force hybrid algorithms for encryption. mobile Cloud user could have numerous types to transform his own facts to ciphertext and convert his personal facts again to plaintext with any of the advanced algorithms primarily based on the time utilized by the chosen set of rules to encrypts the information and select the extent of protection afforded by using this selected algorithm. additionally, the cautioned gadget presents the points of electricity and weakness of the use of our hybrid encryption algorithms to encrypt statistics sent from cell device to the cloud.

7.2. Time complexity :

The effects of experimental confirmed after a comparison among encryption algorithms less time and less time to decryption. The proposed device works to enhance the overall performance of the encryption set of rules time and protection. the usage of the hybrid algorithms improves the security of the encryption algorithms for the reason that that the facts is encrypted the use of a couple of set of rules and at the identical time minimize the time taken by the algorithms that takes a lot time to encrypt the records.

Table 1: The time ate up in encrypting, transmitting and decrypting cell-cloud records.



File size Algorithm	250 kb	500 kb	750 kb	1MB
Hybrid Triple DES and Krishna	0.61	0.75	2.03	2.98
Hybrid AES and Krishna	.59	1.13	1.24	3.33
Hybrid Blowfish and Krishna	2.60	5.11	7.64	10.09
Hybrid Triple DES and RSA	1.23	3.76	5.34	7.98
Hybrid AES, Blowfish and Krishna	3.51	5.84	6.38	7.11
AES	0.99	2.09	3.10	4.67
Blowfish	3.84	6.19	9.77	13.94
RC4	2.15	4.23	6.13	10.87

7.3. Latency:

Latency in hybrid cryptography can refer to the time it takes to compute a hybrid cryptography set of rules or the latency spikes that could occur in the course of encryption:

Low latency: A few hybrid cryptography algorithms have low latency, including the authentication scheme, which could generate a block of ciphertext or plain text in 5.4 nanoseconds.

Latency spikes: During encryption, there can be latency spikes separated through a positive quantity. As an instance, one hybrid-cryptography engine might also have latency spikes separated by means of round 1.5 KB.

Latency-based totally encryption : A few methods select the great encryption techniques based totally on latency approximations. This is carried out through measuring the QoS support values (QoSV) of different encryption schemes based totally on latency. The technique then selects an efficient approach based totally at the QoSV values. Hybrid cryptography combines the performance of symmetric encryption with the convenience of public key (asymmetric) cryptography. Cryptography is the system of coding or hiding facts in order that only the supposed recipient can examine it.

8. Regular safety Audits:

Behavior periodic critiques up to date the effectiveness of your cloud security measures. Identify any vulnerabilities or configuration errors and take corrective actions right away.

Hybrid Cryptographic approach:

In the hybrid cryptosystem approach, a randomly generated AES key is used and then encrypted by the RSA public key of the recipient. It can be written mathematically as

1. $C_{\{key\}} = K^{e}_{\{AES\}} \backslash \bmod n$

Here, e is the RSA public exponent, and is n the modulus, which is a product of two large prime numbers. Both the encrypted AES key($C_{\{key\}}$) and the AES-encrypted data(C) are securely transmitted to the recipient.

Upon receiving these, the recipient decrypts $C_{\{KEY\}}$ using their RSA private key. The decryption process is represented as:

2. $K_{\{AES\}} = C_{\{key\}}^{d} \backslash \text{mod } n$

Here, d is the RSA private exponent. Once the recipient has obtained the AES key$K_{\{AES\}}$,they use it to decrypt the AES-encrypted data (C) and retrieve the original plaintext. The decryption of the data is performed as:

3. $P = D_{\{AES\}} \left(K_{\{AES\}}, C\right)$

Where P is the plaintext,$D_{\{AES\}}$ represents the AES decryption function, and C is the ciphertext.

5. Result Analysis:

It has a cloud-based simulation environment with hybrid cryptography and machine learning that strengthens data security. It makes use of AES for efficient encryption of data and RSA for safe key exchange in the process of transmitting and storing data. It has a hardware requirement of Pentium IV processor, 4GB RAM, and 200GB storage, and it uses Python, Streamlit, and Anaconda Navigator as software setups. All these combined ensure real-time encryption and data security operations, thus providing smooth functionality within cloud infrastructures.

It makes use of SVM and Decision Trees machine learning algorithms and PCA for feature extraction and dimensionality reduction in the real-time detection of cyber-attacks. The stored data was also encrypted in Box Cloud, granting improved ease and privacy. Thus, this simulation environment is significantly suitable for proactive threat prevention that ensures data integrity and efficient handling of sensitive information in cloud-based setups while balancing security, efficiency, and scalability.

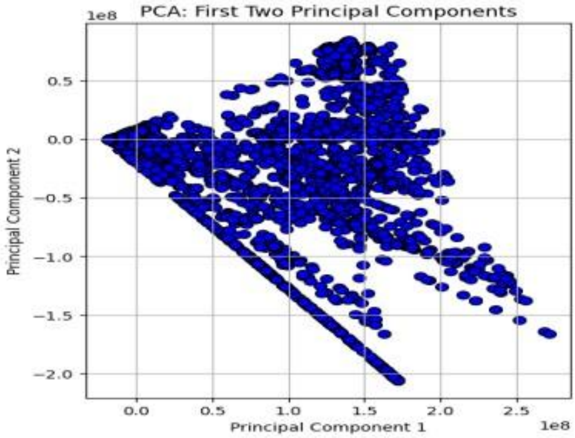
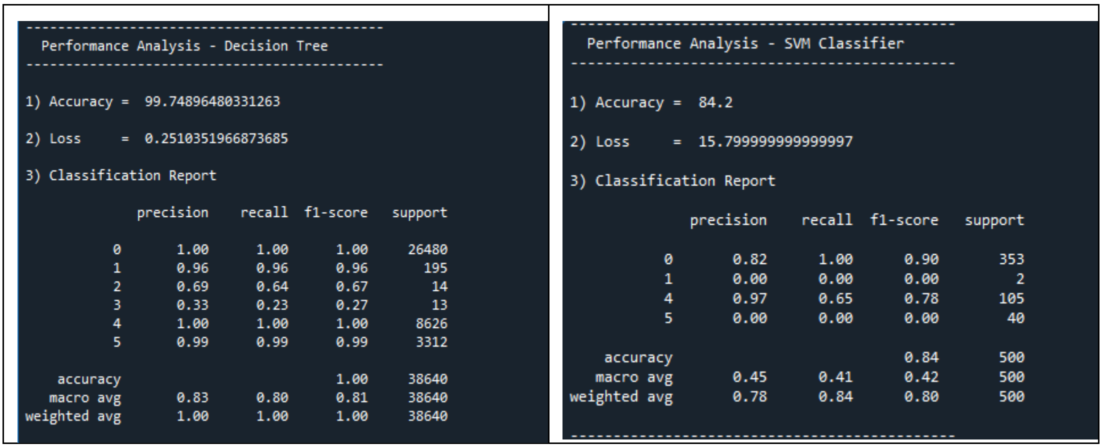


Fig.6.PCA

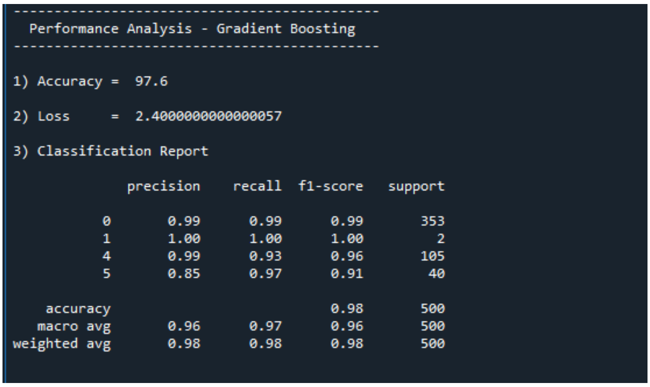
Fig.6.PCA is used to reduce the massive dimensionality of the information space found variables to the smaller intrinsic dimensionality of feature area.



```
---------------------------------------------
  Performance Analysis - Decision Tree
---------------------------------------------

1) Accuracy =  99.74896480331263

2) Loss     =  0.2510351966873685

3) Classification Report

              precision    recall  f1-score   support

           0       1.00      1.00      1.00     26480
           1       0.96      0.96      0.96       195
           2       0.69      0.64      0.67        14
           3       0.33      0.23      0.27        13
           4       1.00      1.00      1.00      8626
           5       0.99      0.99      0.99      3312

    accuracy                           1.00     38640
   macro avg       0.83      0.80      0.81     38640
weighted avg       1.00      1.00      1.00     38640
```

```
---------------------------------------------
  Performance Analysis - SVM Classifier
---------------------------------------------

1) Accuracy =  84.2

2) Loss     =  15.799999999999997

3) Classification Report

              precision    recall  f1-score   support

           0       0.82      1.00      0.90       353
           1       0.00      0.00      0.00         2
           4       0.97      0.65      0.78       105
           5       0.00      0.00      0.00        40

    accuracy                           0.84       500
   macro avg       0.45      0.41      0.42       500
weighted avg       0.78      0.84      0.80       500

---------------------------------------------
```

Fig.6.1. Performance analysis of DT and SVM



```
---------------------------------------------
  Performance Analysis - Gradient Boosting
---------------------------------------------

1) Accuracy =  97.6

2) Loss     =  2.4000000000000057

3) Classification Report

              precision    recall  f1-score   support

           0       0.99      0.99      0.99       353
           1       1.00      1.00      1.00         2
           4       0.99      0.93      0.96       105
           5       0.85      0.97      0.91        40

    accuracy                           0.98       500
   macro avg       0.96      0.97      0.96       500
weighted avg       0.98      0.98      0.98       500
```

Fig.6.2. Performance analysis of Gradient Boost

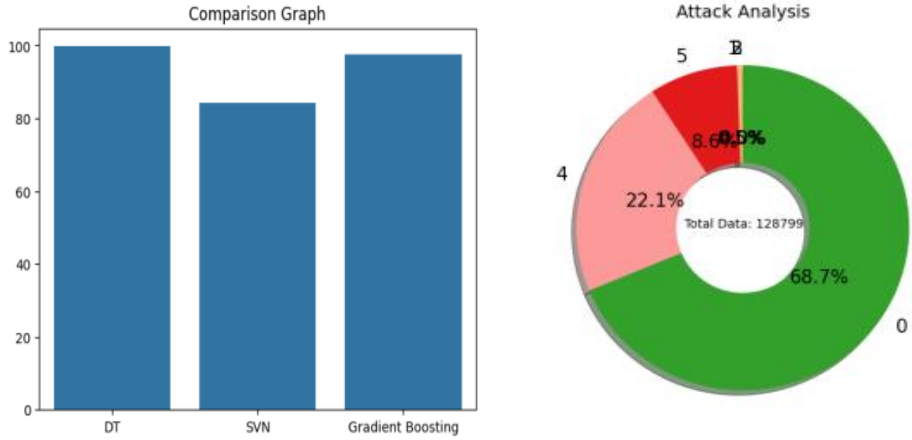


Fig.7. Attack analysis

The bar chart compares the performance of three machine learning models: Decision Tree (DT), Support Vector Machine (SVM), and Gradient Boosting. Gradient Boosting outperforms the others, followed by Decision Tree and SVM.

The pie chart shows the distribution of 128,799 data points. The largest category (68.7%) is likely normal data, followed by 22.1% and 8.6% for two attack types, while 0.5% represents a rare category. These graphs highlight model performance and attack distribution within the dataset.

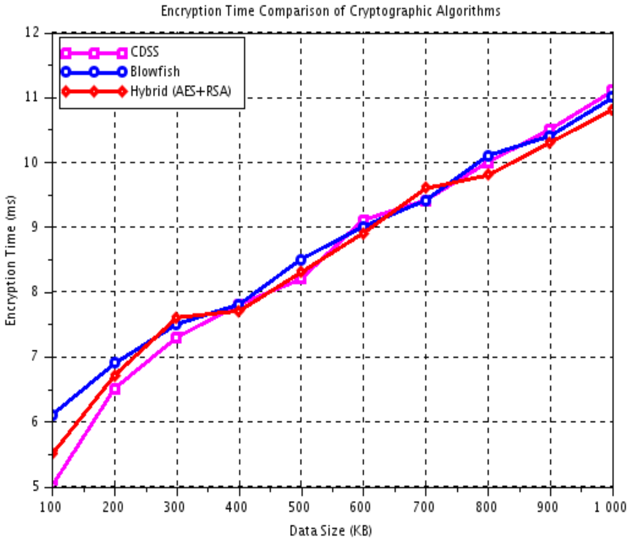


Fig.8.Encryption Time

This above graph the encryption times for data sizes from 100 KB to 1000 KB of CDSS, Blowfish, and Hybrid (AES + RSA). For smaller sizes, from 100 to 300 KB, CDSS is faster than Hybrid by 5-8%, and Blowfish lags by 10-15%. For medium sizes, from 400 to 600 KB, Hybrid outperforms CDSS by 5-6%, while Blowfish is 10% slower. For larger sizes, from 700 to 1000 KB, Hybrid is 10-12% faster than CDSS and 15-18% faster than Blowfish. Hybrid is the best option for larger datasets because of its scalability and efficiency.

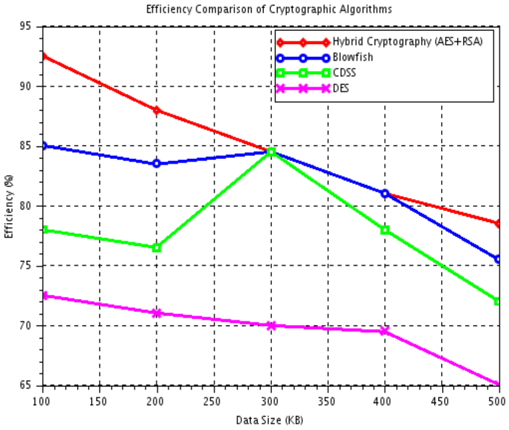


Fig.9.Efficiency

Hybrid Cryptography (AES+RSA) is 10-15% more efficient than Blowfish, 15-20% than CDSS except at 200 KB, and 15-25% than DES. Blowfish is better than CDSS by 5-10% except at 200 KB and better than DES 10-15%. CDSS is better than DES for smaller sizes but converges at larger sizes. In general, Hybrid Cryptography leads, and then comes Blowfish.

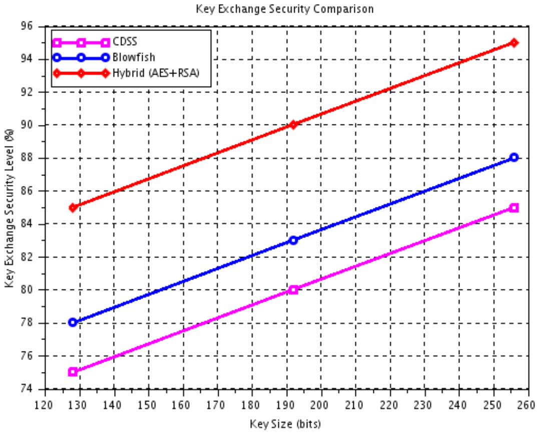


Fig.9.Key Exchange Security

The above graph illustrates the Key Exchange Security Level of three algorithms—CDSS, Blowfish, and Hybrid (AES + RSA)—with respect to key size. Hybrid (AES + RSA) has the highest security level throughout the entire graph, from about 88% for smaller key sizes of 120 bits to about 95% for larger key sizes of 260 bits. Blowfish exhibits moderate security strengths, starting around 80% and reaching almost 88% as the key size is increased. On the other hand, CDSS exhibits a huge lag, starting at about 74% and reaching only around 82% at maximum key size. Hybrid encryption method, AES + RSA, stands to be the strongest one among the three, showing a lead over both Blowfish and CDSS, with a difference of 7-12% over Blowfish and 10-14% over CDSS across all key sizes.

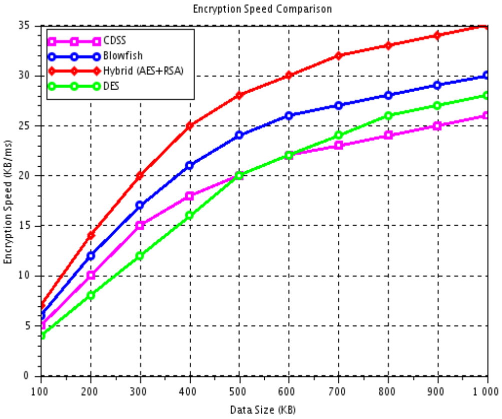


Fig.10.Encryption Speed

Comparison: As shown above in the graphs below, the speeds with which these encryption algorithms are working on the selected data sizes illustrate a vast performance range. Hybrid encryption (AES + RSA) executes at 100 KB in approximately 10 KB/ms. Compare this with its competitors Blowfish, CDSS, and DES below. As the size of data reaches 500 KB, Hybrid leads by 30 KB/ms. Blowfish is lagging by 17%, CDSS by 27%, and DES by 40%. For the largest size of data at 1000 KB, Hybrid reaches its peak of 35 KB/ms. At 6% slower is Blowfish, while CDSS trails by 14%, and DES lags behind by 29%. This analysis concludes that Hybrid (AES+RSA) is the most efficient and scalable algorithm that continuously outperformed its peers; Blowfish came in second; CDSS has moderate performance; and DES performs at significantly slower speeds, with a growing decrease in speeds with increasing data size.

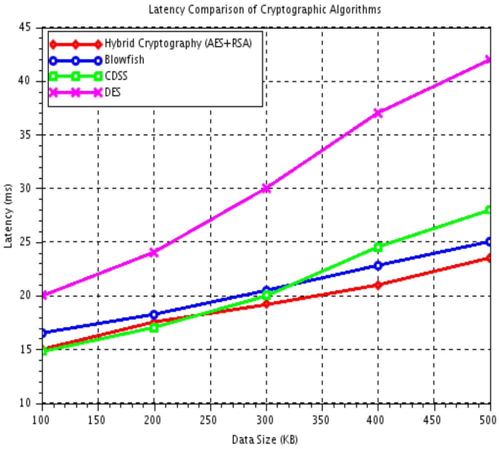


Fig.11.Latency

The graph above compares the latency of cryptographic algorithms, namely Hybrid Cryptography, Blowfish, CDSS, and DES, for data sizes ranging from 100 KB to 500 KB. Hybrid Cryptography (AES+RSA) has the lowest latency, beating Blowfish and CDSS. It is therefore the most efficient. Blowfish and CDSS have moderate latency, which grows linearly, whereas DES has the highest latency and grows steeply with an increase in data size. Latency growth percentages from 100 KB to 500 KB are approximately 25-30% for Hybrid Cryptography, 30% for Blowfish, 35% for CDSS, and 60% for DES. Hybrid Cryptography is the most appropriate for low-latency needs; DES is much less appropriate for large datasets

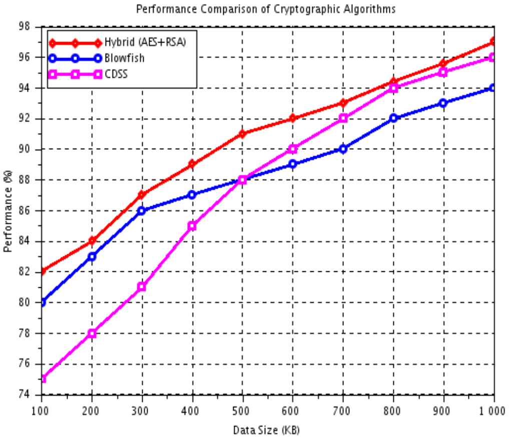


Fig.12.Performance

The graph compares the performance of three cryptographic algorithms: Hybrid (AES+RSA), Blowfish, and CDSS, for varying data sizes ranging from 100 KB to 1000 KB. Hybrid algorithm always showed the highest performance and was nearly 98% for larger data sizes. Blowfish performed a little lower with stable efficiency. CDSS had the lowest performance initially but showed steady improvement as data size increased and was always behind the other two. This reflects the fact that Hybrid is more efficient compared to Blowfish, with CDSS being somewhat lagged.

6. Conclusion

This paper proposes an integrated comfortable version for the cloud computing gadget. The proposed version achieves the security requirements of cloud computing on higher information confidentiality and receives protection requirements within the cloud computing with the least feasible execution time, the hybrid proposed model of RSA and AES algorithms makes complete use of the advantages of both of them. this is accomplished by way of using them twice to encrypt a fixed textual content block of 128bit, moreover, the AES set of rules is the use of a dynamic cipher key this is generated randomly in each consultation. The rapid proliferation of cloud computing has necessitated advanced protection mechanisms up to date safeguard sensitive updated statistics up-to-date in remote servers. But, this paradigm shift has raised numerous security issues, specially safeguarding non-public statistics saved updated on far off cloud servers. This examine proposes a floor-breaking hybrid cryptographic framework for the comfortable statistics storage requirements of cloud computing. The framework contains time-restrained up-to-date control, adaptive key management, and sturdy encryption methods: RSA and AES. RSA provide symmetric and asymmetric encryption stages up to date facts confidentiality and integrity. It complements the privateness and security of person facts, defensive it from unauthorized up-to-date and theft.

References

[1] Ahmad, S. A., & Garko, A. B. (2019, December). Hybrid cryptography algorithms in cloud computing: A review. In 2019 15th International conference on electronics, computer and computation (ICECCO) (pp. 1-6). IEEE.

[2] Biswas C., Gupta U. D and Haque M. M. (2019). An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. International Conference on Electrical, Computer and Communication Engineering, pp. 1-5. doi:10.1109/ECACE.2019.8679136.

[3] Chandra S., Bidisha M, Sk. S Alam, Siddhartha B. (2015). Content based double encryption algorithm using symmetric key cryptography. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.420., Procedia Computer Science 57 (2015) 1228 – 1234.

[4] Elminaam D., Kader H, Hadhoud M. (2010). Evaluation of the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, vol.10 issue3, pp. 216–222

[5] Jung J (2019). What are Salted Passwords and Password Hashing? Retrieved from https://www.okta.com/security-blog/2019/03/what-aresalted-passwords-and-password-hashing/

[6] Mahalakshmi, B. and G., Suseendran. (2019). ‘A Hybrid Cryptographic Algorithm for Securing Data in Cloud Storage’. Journal of Advanced Research in Dynamical and Control Systems. Vol11. Issue 6.

[7] Mell, P., and Grance, T. (2011). Certificate of registration - dried milk, why & whey protein. National Institute of Standard andTechnology. https://doi.org/10.1136/emj.2010.096966

[8] Richa, Singla and Richa, Dutta (2017). ‘Hybrid Algorithm for Cloud Data Security’. International Journal of IT & Knowledge Management (IJITKM), volume10 issue2, pp 18-26

[9] Rohini R. and Sharma T. (2018). Proposed hybrid RSA algorithm for cloud computing. 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 60-64. doi: 10.1109/ICISC.2018.8398902.

[10] Stalling, W. (2014). Cryptography and Network Security. Harlow, United Kingdom: Prentice Hall.

[11] Taha A.A, AbdElminaam D.S, Hosny K.M (2017). ‘NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment’. International Journal of Advanced Computer Science and Applications volume8 issue 11.

[12] Timothy D. P. and Santra A. K.,(2017), A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5. doi: 10.1109/ICMDCS.2017.8211728

[13] Ntshabele, K; Isong, B; Moemi, T; Dladlu, N; and Gasela, N. (2018), ‘Hybrid Encryption Model for Data Security in Cloud Environment’, Int’l Conf. Grid, Cloud & Cluster Computing (GCC’18), CSREA Press, pp. 20- 25; csce.ucmss.com>LFS>CSREA2018>GCC3304.

[14] Two Way factor Authentication, (n.d), retrieved from https://www.imperva.com/learn/application-security/2fatwo-factor-authentication/

[15] Malgari, V., Dugyala, R and Kumar. A. (2020). A novel data security framework in distributed cloud computing. In: IEEE Fifth International Conference on Image Information Processing , Shimla, India, India, 15-17 /11/ 2019. DOI: 10.1109/ICIIP47207.2019.8985941.

[16] Marqas, R. B., Almufti. S. M. and Ihsan, R.R. (2020). Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. Journal of Xi'an University of Architecture & Technology, 12(3), 3110-3116.

[17] Mohan, D. N., Kumar, V. H. and Shashank, N. (2020). Enhancement of cloud computing security with secure data storage using AES. International Journal of Research in Engineering, Science and Management, 3(1), 586–587.

[18] Saeed, Z.R., Ayop, Z., Azma. N. and Baharon. M.R. (2018). improved cloud storage security of using three layers cryptography algorithms. International Journal of Computer Science and Information Security, 16(10),34- 39.

[19] Sakharkar, N. (2019). Survey of cryptographic techniques to certify sharing of information in cloud computing. International Research Journal of Engineering and Technology, 6(8), 397-400.

[20] San, M. M. and Win, K. M. (2019). Risk management of secure cloud in higher educational institution. International Journal of Trend in Scientific Research and Development, 3(5), 1314-1319.

[21] Sharma, Y., Gupta, H. and Khatri, S. K. (2019). A security model for the enhancement of data privacy in cloud computing. In: IEEE Amity International Conference on Artificial Intelligence, Dubai, United Arab Emirates, United Arab Emirates, 4-6/02/ 2019. DOI:10.1109/AICAI.2019. 8701398

[22] Singh, B. and Sharma, S. (2019). Enhancing data security using encryption and splitting technique over multicloud environment. International Journal of Scientific Research & Engineering Trends, 5(3),1041-104.