Hybrid DES-RSA Model for the Security of Data over Cloud Storage

Rajan Kumar Yadav[1], Munish Saran[2], Pranjal Maurya[3], Sangeeta Devi[4], Upendra Nath Tripathi[5]

[1,2,3,4,5] Department of Computer Science, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur, Uttar Pradesh, India

Abstract:

Cloud computing is a novel business strategy. Over the past several years, the idea of cloud computing has matured, becoming one of the most rapidly expanding business concepts in the IT sector. The capacity of cloud computing to supply consumers with elastic, dependable, and reasonably priced services on demand has contributed to its meteoric rise in popularity in recent years. Since cloud computing provides users with scalable, on-demand services while requiring less investment in infrastructure. Client data and computations must be protected from both internal and external threats in order to allay fears that cloud computing is inherently insecure. This is due to the fact that cloud users get the required information from distant cloud servers that are not under the direct management of the data owners and that the data owners store their sensitive information on remote hosts. The client has the option of implementing security measures such as firewalls, VPNs, and other perimeter-based controls to safeguard their information. Data stored in the cloud raises privacy and security concerns since it is not located on the client's premises. Therefore, data security is a major focus area in the cloud computing industry. To address these issues with cloud data security, we have developed solutions and strategies. Collectively, the models we've offered to ensure data security, privacy, and integrity constitute comprehensive principles for bolstering cloud data security. Cloud security risks and privacy issues, as well as the types of assaults and threats to which clouds are susceptible, are all addressed in the models. We've also solved the problem of how to store data on the cloud effectively. Additionally, we propose a general security model for cloud computing that might assist in satisfying its security requirements and safeguarding clouds from different hazardous behaviors

Keywords: Cloud Computing, Crytography, DES, RSA, Cloud Security, Authentication.

DOI: 10.24297/j.cims.2023.7.12

1. Introduction

Protection of client data and computations against a variety of assaults by the cloud provider and outsiders is a major issue in cloud computing. This is due to the fact that cloud users lack the authority to independently build, install, and manage security solutions. Despite cloud

computing numerous benefits, this new model comes with several drawbacks that cloud users, persons or organizations leasing cloud services should think about before making the leap. Some of them will be talked about from here on out [1].

Information saved or processed by the cloud is accessible first and foremost by the cloud service provider (CSP), who offers and operates the cloud infrastructure.

Second, because CSPs optimise their usage of resources by dividing them among several consumers. Customers of the CSP, with whom you share cloud resources and who may attempt theft or other forms of data exploitation, pose this risk.

Third, employing cloud services via the same old channels and protocols leaves them open to the same old assaults and breaches that are already commonplace from the outside. Researchers have found that the majority of attacks on cloud-hosted software use tried-and-true techniques, such as targeting publicly accessible web services [2].

Since cloud computing is inherently suspect, it appears that cloud users will have to demonstrate some level of trust in their CSP. Providers of cloud computing services face the issue of bringing the level of mistrust down to a manageable level. In the real world, cloud data integrity research is also important for reasons beyond only privacy. Integrity is also vital because there are crimes that can be committed for illegally accessing transmitted data. The transition from on-premises to cloud-based servers should be transparent to users [3].

Validity and authenticity of the users must also be confirmed. Signatures and witnessing are common tools for achieving non-repudiation (the inability to deny having taken a particular action; for example, if you buy a share, you should not later deny it), which is a desirable property in the real world (although reputation is even more important in this scheme). Data privacy, integrity, and authenticity may all be strengthened by using cryptographic techniques, which are increasingly finding widespread use. Maintaining the privacy of cryptographic keys is a significant difficulty for real-world cryptosystems since their security depends on them. While cryptography cannot guarantee safety by itself, it can provide a substantial safeguard. It is of importance to us to both render information that was previously understandable unintelligible (by scrambling it) and to render information that was previously incomprehensible

understandable. Encryption and decryption are the most common names for these processes [4].

The cryptographers, who create the tools we use to encrypt and decode information, are always at odds with the cryptanalysts, who crack codes. As a group, they tend to play on the same team and lodge together for added security. Plaintext refers to information in its naturally comprehensible state. The encrypted communications created by this process are known as cipher text and are unreadable by the adversary. The plaintext and cipher text alphabets in current computer-based cryptography are the basic {0, 1}, although in the past they were the alphabet [5].

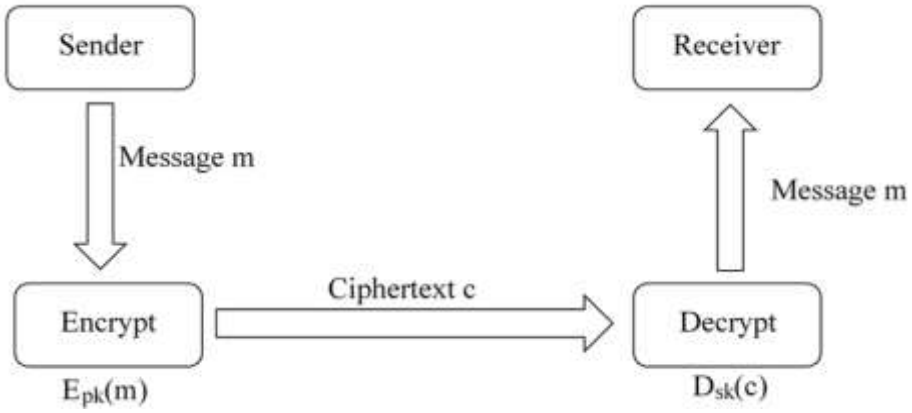

Fig.1. Process of Cryptography

Figure 1 depicts what appears to be a typical block diagram of the procedure. Private, or symmetric, key cryptography is one method, whereas public key cryptography is another. Keys K and K-1, which are used for encryption and decryption respectively, are identical in the private key, or can be derived from one another with little effort. Both keys in a public-key cryptosystem are unique, and it takes a lot of work (and additional information) to figure out which one comes from the other [6].

In the last 30 years, public key cryptography has emerged, with many inventors (. The use of private keys in cryptography goes back for further in time.

2. Related Work

The rise in popularity of cloud computing in the modern period has prompted a slew of academic investigations. As the number of people using the cloud grows, so does the importance placed on ensuring the safety and effectiveness of the services provided by the data

centre. Several methods have been proposed by the research community to make cloud computing safe and effective. Authors in [7] noted that while significant strides had been made towards understanding the performance behaviors of distinct Cloud services, a wide range of outstanding concerns remained in each category and required additional exploration. A Quality-of-Service (QoS) driven strategy to cloud computing was presented in [8]. Quality of service (QoS) has also been a major area of attention, as achieving it in a cloud setting is not easy due to the wide variety of clients and their unique service needs.

Quality-of-Service (QoS) has been identified by Subha et al. in [9] as one of the most important aspects of cloud computing. Constantly picking cloud services based on QoS needs is a difficult decision. Both cloud service providers and cloud customers must meet these conditions. By focusing on the significance of data integrity methods for outsourced data, Faheem Zafar et al. in [10] want to improve our comprehension of security concerns related to cloud storage. The cloud storage industry has benefited from the offered taxonomy of existing data integrity techniques. In addition to a thorough breakdown of potential security threats and their countermeasures, a comparison of the current setup is presented.

The complexity of intrusion detection has increased in terms of computational effort, storage requirements, and the likelihood of obtaining optimal classification solutions in a readily available sequential computing environment, as discussed by Natesan et al. in [11]. A cryptography-based security solution for the cloud was proposed in 2017 by Laurence T. Yang et al. They compared their experimental findings to their original concept of the RSA algorithm, which is used in public-key cryptography. The RSA technique had been frequently employed in cloud computing for possible data protection.

Academics and researchers have taken notice of the major security and privacy problems in that sector as outlined by authors in [12]. Various researchers have recognized and presented security solutions in the literature, despite the various obstacles. Finally, unanswered questions are offered after a comparison of the works is made according to various privacy and security standards. Risk levels and attack types are also highlighted in a unique approach to special security assaults in cloud services given by Syed Asad Hussain et al. in [13]. Risk levels range from "high" to "medium" to "low." Stronger risk levels necessitate more stringent multi-tenancy, authentication, authorization, data encryption, and security measures. Dinh-Mao Bui et al. in [14] made an effort to offer a resource orchestration system that uses less energy in the cloud. The

suggested method relied on the Gaussian process regression technique to make predictions about resource use in the subsequent period. A technique for reversible information stowaway in encoded images was proposed by [15]. It was suggested that an algorithm be developed that would first identify the region of interest and then the noisy pixel. Authors in [16] provided an overview of the economy, and a new production model called Cloud production Mode (CMM) was presented not long after. CMM offered extensive production capacities and resources as manufacturing services.

3. Proposed Work

The proposed algorithm employs two different kinds of encryption, both of which will be briefly discussed below:

DES Algorithm

The DES algorithm employs a 64-bit key length and a 64-bit block size. Each byte of code also has a parity bit added, increasing the effective key length to 56 bits. Eight bytes are used to represent the key, and they must all be in an odd parity state. Triple DES (TDES), Two-Times DES (TDES), and Three-Times DES (TDES) are all DES versions that use more than one key. Although it is slow, TDES is secure enough for most uses. The maximum cryptographic security of DES is still 64 bits, and this holds true even if round sub-keys are chosen arbitrarily rather than derived from a key.

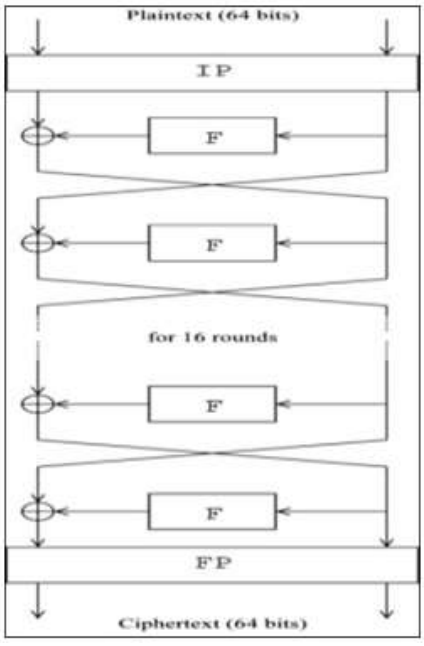

Fig.2. DES Process

There are 16 distinct procedures in the treatment protocol. Although they have no cryptographic relevance, IP and FP variants on that point are also permitted for the sake of simplicity when loading and unloading blocks from hardware. The first bit of output comes from the 58th bit of input, the second bit from the 50th bit, and so on down to the final bit of output coming from the 7th bit of input, at which point permutations begin. Each new permutation improves upon the one before it. As can be seen in Figure 1, a Fiestal function requires the main block to be split in half along the 32-bit boundary. The one exception in the Fiestal design is that the sub-keys are utilized in the opposite sequence for decryption. Everything else on the agenda remains the same. The F-function works by first scrambling half of a block using a subset of the keys, then mixing that half with the other half, and then exchanging the two halves before moving on to the next cycle. After one full rotation, the two halves are swapped.

RSA Algorithm

In 1978, MIT's Rivest, Shamir, and Adleman presented the RSA algorithm. The RSA public-key cryptosystem is widely used because it uses exponentiation over integers modulo a prime number. When it comes to key exchange, digital signatures, and encrypting whole blocks of data, This is the most well-introduced system of public key cryptography. RSA employs both a key and an encryption block of varying sizes. It is a number-theory based block encryption scheme, making it asymmetric (using public keys). To generate the public and private keys, it requires two prime integers. The encryption and decryption processes need two distinct keys. The communication is encrypted by the sender with the recipient's public key, and may be decrypted by the recipient using his private key. Key creation, encryption, and decryption are the three main components of an RSA operation. Due to its design flaws, RSA was not chosen for this commercial application. When using the lowest feasible values for a and b, the encryption approach is too susceptible to random probability theory and side channel assaults. When using large a and b values, however, the algorithm's performance degrades and its execution time increases relative to that of DES.

Proposed Model

The proposed architecture has been designed to safeguard data at every stage of the cloud computing lifecycle, from storage to transmission. Therefore, several procedures and methods are used to prevent unwanted access to the sensitive data. There are four stages to the proposed structure. In the first step, the user registers with the CSP. The second step is putting the information away in a cloud service. In the last stage, authentication is handled during the data

retrieval request. The last step involves returning the data to the authorized user after it has been successfully recovered from the cloud and having that data's integrity verified.

First Phase: Initial Cloud User Registration with Cloud Service Provider

First, the user must register with the cloud service provider by supplying the provider's credentials (username, password, registered mobile number), as shown in Figure 3. The CSP will store the resulting hash code from hashing the password using the MD5 algorithm. The CSP database will be safe against account hijacking and insider attacks if password hashes are stored there.This policy prohibits unwanted access to the user account by having the CSP produce an OTP after confirming the user details and sending the information to user working on cloud, who then re-enters the OTP and has it validated by the CSP. The additional step of entering a CAPTCHA will further fortify the system against password-cracking bots. This idea guarantees that the user data is entered by hand.

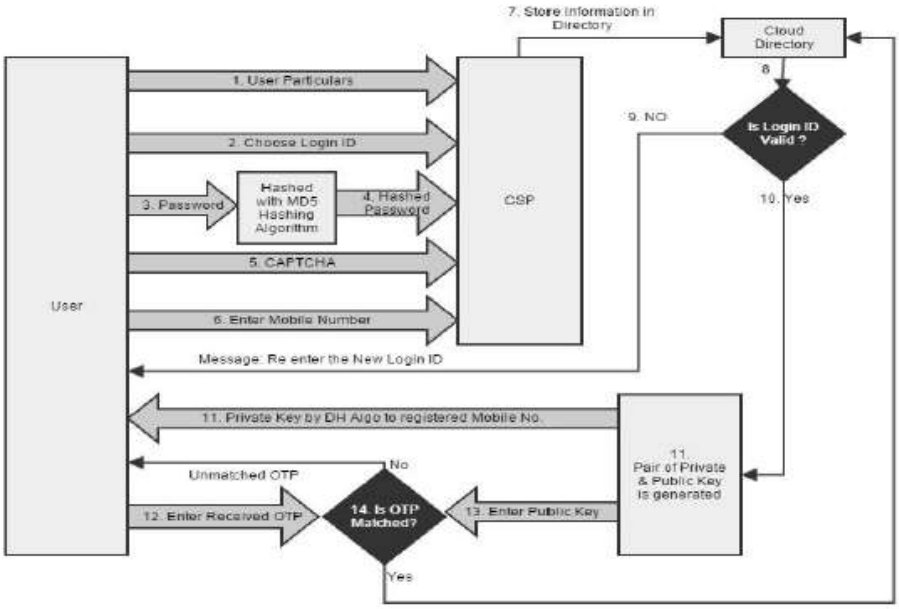

Fig.3. Cloud User Registration

Second Phase: Data Storage on the Cloud

This phase, represented in Figure 4, comprises uploading encrypted data to a remote server. This process is divided into three distinct phases: user-side encryption, hash code generation, and CSP-side encryption.

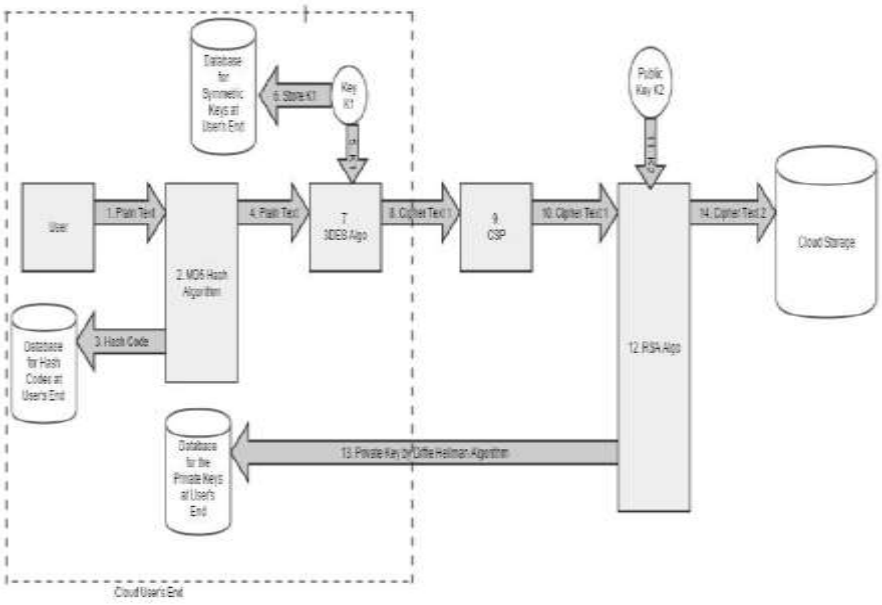

Fig.4. Data Storage on cloud

Now that you've signed up with a CSP, you can begin moving your files to the cloud. Data is encrypted with a 3DES symmetric key technique, and the user saves the created public key in their own database, corresponding to the encrypted file's unique identifier. The process of converting plain text into ciphertext 1 may now begin. The 3DES algorithm is used because it is much more effective than the DES method.Each user may generate their own MD5 hash code and save it in a database with the file ID to ensure the data is authentic. When data is retrieved from the cloud, its integrity is checked using a hash algorithm, a one-way cryptographic approach that creates a hash code that changes if even a single character in the file is changed. This prevents data loss or corruption due to human error.

The CSP then applies RSA, another asymmetric key cryptography technique, on the file after receiving cypher text 1. This cryptography procedure generates both a public and private key. An authorised user receives the public key created by RSA, which is re-encoded into cypher text 1 using the Diffie-Hellman technique, and the private key, which corresponds to the public key, is securely conveyed back to the user, who stores it in a database using the same file ID. Adding a second layer of encryption to all stored files allows us to fix the flaws of the first.

Third Phase: Access to data requires user authentication

Figure 5 illustrates the CSP's need to verify the user's identity before allowing access to the data. Cloud service providers typically require users to enter their Identification (username), Password, and Captcha. The CSP compares the information provided with what is recorded in its cloud directory, ensuring the authenticity of the passed credentials. An OTP is sent to the user's registered cellphone number by the CSP when verification is complete. The user re-enters the OTP into the CSP for verification purposes.

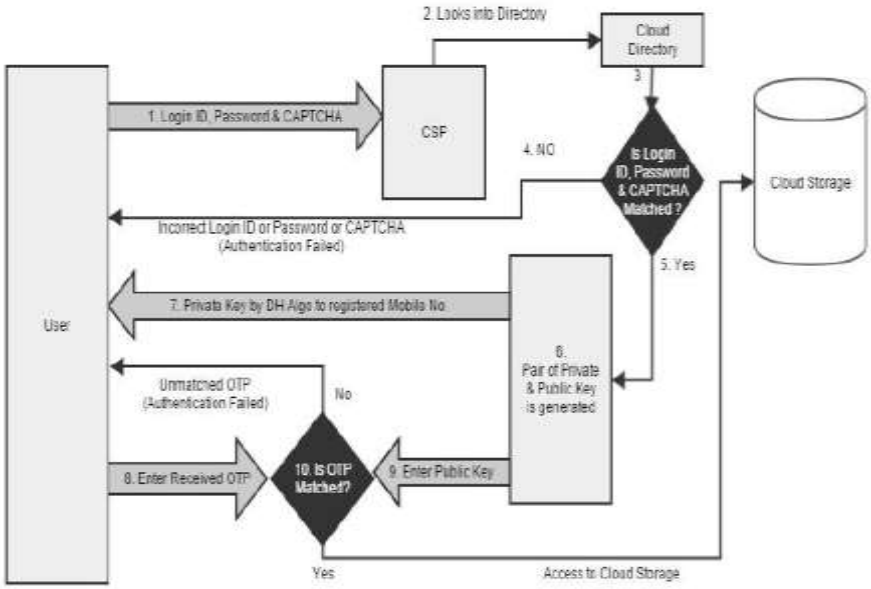

Fig.5. Authorization of the Data Requester

Fourth Phase: Information Recovery and Assurance of Authenticity

In cases when data is obtained from the CSP end in an encrypted format, the authorized user can look up the corresponding private key, hash code, and public key in their own database using the recovered file ID as shown in figure 6.. The user first deciphers cipher text 2 using their RSA private key, resulting in cipher text 1, and then deciphers cipher text 1 using their 3DES symmetric key, resulting in plain text. The plain text that was retrieved is then hashed using the MD5 technique, and the resulting hash value is compared to the key values that were previously recorded; if they match, the process ends; otherwise, the CSP is notified of the legal process.

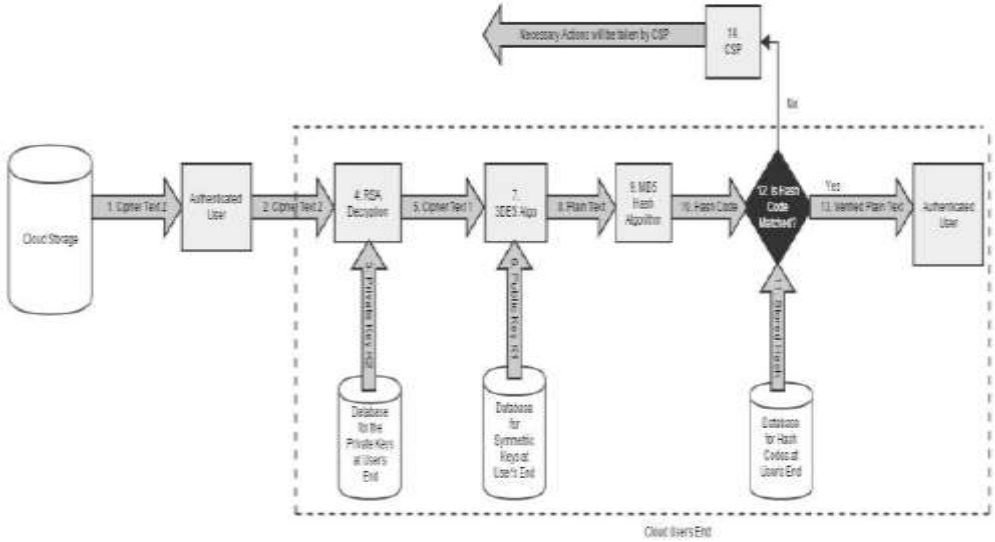

Fig.6. Information Recovery and Assurance of Authenticity

Therefore, consumers may feel safe entrusting their data to the cloud if they use the proposed strategy. A third party intercepting the data in transit would only be able to decipher cypher text 1, as the public key is kept securely on the premises of the authorized user. It would take a long time, maybe years, to crack the key.

The proposed method requires a private key and public key, both of which must be safely stored on the premises of the authorized user. The data is stored as cypher text 2, making it unusable without both the private key and public key, even if an unauthorized user were to obtain it from cloud storage.

Data stored in off-site cloud storage using the proposed method would be accessible only in cipher text 2 formats, which would be worthless to an unauthorized user without the private key and public key, which are in the safe possession of the authorized user.

4. Results And Discussion

Three separate security solutions are offered for sustaining the protection and integrity environment of cloud data in order to maximize control of data possessor over cloud data stored in some faraway place. The proposed model is shown to be highly secure and privacy conscious in both their operation and efficiency across all cloud settings.

To save time and effort, we first divide the data into layers according to how sensitive it is. Then, for each layer of data, we apply and analyze a variety of encryption method permutations. It has been determined that the proposed algorithms are effective in protecting the confidentiality and integrity of the archived data.

There has been extensive research into the efficacy of the proposed algorithm against a wide range of common security threats, and the results show that it stands up well to the most common of these attacks (listed in Table 1).

Table 1. Comparison of Proposed Model with DES and RSA Algorithm Resistance against different Attacks

Sr.	Attacks	DES	RSA	Proposed Model Resistance
1	Denial-of-Service Attacks	Below Average	Average	Good
2	Account Hijacking	Below Average	Average	Good
3	User Account Compromise	Below Average	Good	Good
4	Cloud Malware Injection Attacks	Below Average	Average	Good
5	Insider Threats	Below Average	Good	Good
6	Side-Channel Attacks	Below Average	Average	Good
7	Cookie Poisoning	Absent	Absent	Good
8	Security Misconfiguration	Absent	Absent	Good
9	Insecure APIs	Absent	Below Average	Good
10	Cloud Cryptomining	Absent	Good	Good

Table 2. Comparison of proposed method performance with DES and RSA on the basis of speed and processing cost

Sr. No.	Parameters	DES	RSA	Proposed Model
1	Speed	Slow	Moderate	Fast
2	Computational Cost	Nominal	Most	More

5. Conclusion And Future Work

To address the issue of data security in the cloud, this research proposes a novel hybrid method. This method protected the privacy and integrity of data during transmission and rest, when cloud data is most vulnerable to assaults, and maximum data ownership and control in the cloud has been achieved.. Data privacy, integrity, and verifiability are all being protected with the use of cryptographic methods. Maintaining the privacy of cryptographic keys is a significant difficulty for real-world cryptosystems since their security depends on them. The suggested approach makes use of not one but two forms of encryption. This proposed solution offers a variety of encryption methods to ensure the safety of data at the endpoint of the cloud service provider. Well-known symmetric cryptography methods like 3-DES and hashing methods like MD5 and asymmetric cryptography methods like RSA and key exchange methods like Diffie Hellman were all incorporated into the policy that was implemented. Most attacks discovered so far on cloud data during transmission and storage have been determined to have no effect on the proposed method. One possible approach is to apply the suggested idea to both completely homomorphic and partly homomorphic encryption methods, which would allow for the same processing to be carried out on encrypted material while yielding identical results to those obtained when processing plain text.

References

1. P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in *IEEE Access*, vol. 8, pp. 131723-131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

2. Soni, D., Srivastava, D., Bhatt, A., Aggarwal, A., Kumar, S., & Shah, M. A. (2022). An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol. Mathematical Problems in Engineering.
3. Kaja, Durga & Fatima, Yasmin & Mailewa, Akalanka. (2022). Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. International Journal of Research Publication and Reviews. 713-720. 10.55248/gengpi.2022.3.2.8.
4. Bhargav, A. & Manhar, Advin. (2020). A Review on Cryptography in Cloud Computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 225-230. 10.32628/CSEIT206639.
5. Srivastava, D., Kumar, A., Mishra, A., Arya, V., Almomani, A., Hsu, C. H., & Santaniello, D. (2022). Performance Optimization of Multi-Hop Routing Protocols With Clustering-Based Hybrid Networking Architecture in Mobile Adhoc Cloud Networks. International Journal of Cloud Applications and Computing (IJCAC), 12(1), 1-15. http://doi.org/10.4018/IJCAC.309932.
6. S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377.
7. Srivastava, D., Sharma, V., & Soni, D. (2019, April). Optimization of CSMA (Carrier Sense Multiple Access) over AODV, DSR & WRP routing protocol. In 2019 4th international conference on internet of things: Smart innovation and usages (IoT-SIU) (pp. 1-4). IEEE.
8. Bruno Guazzelli Batista, Carlos Henrique Gomes Ferreira, Danilo Costa Marim Segura, Dionisio Machado LeiteFilho & Maycon Leone MacielPeixoto 2017, 'A QoS-driven approach for cloud computing addressing attributes of performance and security' , Future Generation Computer Systems, vol. 68, pp. 260-274.
9. Subha, M &UthayaBanu, M 2014, 'A survey on QoS ranking in cloud computing,' , International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 2, pp.293-300.
10. Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, Fuzel Jamil, A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends, Computers & Security, Volume 65, 2017, Pages 29-49, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2016.10.006.

11. Natesan, P, Rajalaxmi, RR, Gowrison & Balasubramanie, P 2017, 'Hadoop Based Parallel Binary Bat Algorithm for Network Intrusion Detection', International Journal of Pattern Programming, vol. 45, no. 5, pp 1194-1213.
12. Salman Iqbal, Laiha, Mat Kiah, BabakDhaghighi, Muzammil Hussain, Suleman khan, Muhammad Khurram Khan & Kim-Kwang Raymond Choo 2016, 'On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service', International Journal of Network and Computer Applications, vol. 74,pp. 98-120.
13. Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja & KhurramShahzad 2017, 'Multilevel classification of security concerns in cloud computing', Applied Computing and Informatics, vol.13, no. 1, pp. 57-65.
14. Dinh-Mao Bui, YongIk, Yoon, Eui-Nam, Huh, SungIk Jun & Sungyoung Lee 2017, 'Energy efficiency for cloud computing system based on predictive optimization', Journal of Parallel and Distributed Computing, vol. 102, pp. 103-114.
15. Durfi Ashraf & Sayiema Amin 2016, 'Information hiding based on optimization technique for Encrypted Images', International Research Journal of Engineering and Technology (IRJET), vol. 03, no. 01, pp. 1-6.
16. Prabhu, A & Usha, M, 2018 'A Secured best data centre selection in cloud computing using encryption techniques', International Journal of Business Intelligence and Data Mining (Accepted for publication) DOI: 10.1504/IJBIDM.2018.10007299.