I.J. Wireless and Microwave Technologies, **2023, 5, 48-59**
Published Online on October 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.05.05

Enhancing the Cloud Security through RC6 and 3DES Algorithms while Achieving Low-Cost Encryption

Chandra Shekhar Tiwari*
Department of Computer, Science and Engineering, Birla institute of technology Mesra, Ranchi, India
E-mail: tiwaridalton@gmail.com
*Corresponding Author

Vijay Kumar Jha
Department of computer science & Engg, Birla institute of Technology Mesra, Ranchi, India
E-mail: vkjha@bitmesra.ac.in

Received: 25 December, 2022; Revised: 27 February, 2023; Accepted: 18 April, 2023; Published: 08 October, 2023

Abstract: Cloud computing is a cutting-edge system that's widely considered the future of data processing, making cloud computing one of the widely used platforms worldwide. Cloud computing raises problems around privacy, security, anonymity, and availability. Because of this, it is crucial that all data transfers be encrypted. The overwhelming majority of files stored on the cloud are of little to no significance while the data of certain users may be crucial. To solve the problems around security, privacy, anonymity, and availability, so we propose a novel method for protecting the confidentiality and security of data while it is being processed by a cloud platform. The primary objective of this study is to enhance the cloud security with RC6 and 3DES algorithms while attained low cost encryption, and explore variety of information safety strategies. Inside the proposed system, RC6 and 3DES algorithms have been used to enhance data security and privacy. The 3DES has been used to data with a high level of sensitivity to encrypt the key of RC6 and this method is significant improve over the status quo since it increases data security while reduce the amount of time needed for sending and receiving data. Consequently, several metrics, such as encryption time, false positive rate, and P-value, have been determined by analyzing the data. According to the findings, the suggested system attained less encryption time in different file size by securely encrypting data in a short amount of time and it gives outperformance as compared to other methods.

Index Terms: Cloud computing, machine learning, cryptography, encryption, Random Forest, 3DES, RC6

1. Introduction

The provision of cloud services via the use of cloud computing. When information is accessible remotely, applications may then be run using the cloud computing approach. There are three layers of services that are used to characterize “cloud computing: infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS).” Users get access to storage and a variety of visual tools thanks to IaaS. The advents of AI, the IoT, and the mobile internet have all led to the proliferation of data [1, 2]. Users are provided with frameworks through which they may enhance cloud hosting applications in order to construct, utilize, analyze, and administer theorem services via SaaS. PaaS enables customers to access services and applications from any location, at any time, and using any device that can access the internet. People andbusinesses alike are increasingly drawn to cloud computing as a means of offloading their data storage needs [3].As a consequence, cloud storage has expanded significantly in cloud computing [4,5]. Cloud storage may freeup a substantial amount of local processing power by conserving local storage space. Data loss, privacy leaks,and security assaults are only some of the possible downsides of cloud storage [6,7].The user does not control the outsourced data. The integrity of cloud users’ data may be jeopardized ifthe cloud deleted infrequently-used or frequently-repeated data to conserve space. With limited auditingcapabilities, it is hard for the majority of users to determine whether their cloud-stored data are still complete.The problem may be fixed if the user has confidence in a third party to examine the data and report on itscompleteness, accuracy, and consistency. Cloud storage users with shared services should conduct integrityaudits on their cloud storage accounts. Any misbehaving member within a group may threaten other groupmembers’ data security[8-10].

Data security is a big concern because the data are being stored by a third party. The danger is great if users collect information in an open and honest way, and storage also offers a tool for backup.With cloud computing, resources and services are made available to the user at their recommendation and convenience.Integrity auditing strategies [11-13] are constantly being introduced. Public key infrastructure (PKI)-based group data integrity verification has serious security issues and a large computation cost. Most of these options also fail to address secure key management or safeguards for cloud-based data storage.However, previous research has only addressed data security during the cloud storage and retrieval phases, leaving the data open to hacker attacks throughout the upload and download phases.Data and the key should be encrypted toreduce risk and maintain privacy. Keeping data and keys private allows for easier auditing of data given by different sources, making it crucial to develop a robust encryption method [14,15].Multiple parties' shared information applies to a variety of applications, particularly in collaborative circumstances. In federal education, for instance, machine learning has led to effective answers for problems like collaborative learning and parallel computing. Due to a lack of cryptography tools, however, many machine learning strategies are unable to protect privacy [16]. Few solutions [17,18] that combine encryption approaches fail to address CSP-user cooperation.

The primary objective of this paper is to enhance the cloud security through RC6 and 3DES algorithm while low cost encryption. The major limitation in cloud security are as follows: privacy and security of data, service availability, vendor lock in and interoperability, absence of proper services level agreement, performance instability, lack of scalable storage, and latency of network. To overcome the aforementioned difficulty, this work proposes an integrity auditing approach. The following are the primary contributions and major objectives as follows:A new approach based on Cryptography and Machine Learning is presented to enable the safe transmission of data between cloud users. To propose a Random forest classifier for classifying the data according to its sensitivity.By using theRC6 and the 3DES algorithm in a cloud setting, the most critical security criteria known as confidentiality and security have been satisfied.To protect the integrity of data, the MD 5 method for digital signatures has also been presented. Finally, the performance of the proposed technique is equated with existing model. The rest of the paper is designed as follows: section 2 discussed literature work. Section 3 explains the proposed approach methodology and section 4 performs the experimental analysis and results in discussion. Finally, the paper is concluded in section 5.

1.1. Problem Formulation

Deletion of information, lack of control, improper storing, etc., are just a few of the privacy concerns with cloud computing. Since maintaining the privacy and security of one's information is crucial, these concerns provide a serious roadblock to the widespread use of cloud-based computing services. Once a client uploads content to the internet, he needs to know that it will be secure and accessible only by authorized parties. The confidentiality of the user's data could be jeopardized if it were to become accessible to either unauthorized parties or legitimate users as a result of a bug or fraudulent alteration. Some of the problems faced in securing data in the cloud are as follows:

- Because of the widespread use of the World Wide Web to transmit this information, its protection has been identified as a serious issue. Authenticity, verification, and secrecy are only a few of the emerging cloud computing infrastructure issues.
- Clients are not given a wide variety of customizable privacy settings.
- Expensive authentication process.
- Sharing document is expensive.

In light of the aforementioned drawbacks, we have set our sights on the following goals:

a). Data Integrity
b). Verification with very less cost
c). Lightweight implementation

In this research, we propose a novel method for protecting the confidentiality and security of data while it is being processed by a cloud platform.

1.2. Objectives

The following are some of the most important results from this study:

- A new approach utilizing encryption and a Random Forest algorithm is developed to enable the safe transfer of data between clients in a cloud computing system.
- To propose a Random forest classifier to classify the data based on their sensitivity.
- Authenticity and privacy, the primary concerns of cloud computing, have been addressed by the implementation of the RC6 and 3DES algorithms.
- Information consistency has also been addressed with the introduction of the MD 5 cryptographic authentication procedure.

2. Literature Review

When it comes to cloud computing infrastructure, several studies had been conducted as of now. Various writers, with users' safety as their priority, had proposed various methods for achieving this goal.

ThandaiahPrabu et al., 2022 [19] offered a mechanism for real-time material accessibility and retrieval updates. They suggested using a term evaluation system to encode the messages and presented a cipher strategy that could handle several information streams simultaneously. In this work, we describe a new Multi-Data Handling Cipher Policy (MDHCP) and show how it may be utilized to create indexes and searches. The Greedy aided Depth First Search (DFS) method is a fast, multiple keyword, ranked search mechanism that is built on a tree-based data structure index.The suggested method employs a depth-first approach on a tree-based architecture to perform simultaneous keyword-based score investigations quickly. The conclusion section demonstrates how effective the suggested method is, and the graphical demonstrations demonstrate how the proposed method may keep data secure while it is being stored in the cloud environment.

Zhou et al., 2021 [20] presented an N-variant architecture for a safe cloud storage solution for CSP. Specifically, researchers spoke about using SecIngress, a platform for building API gateways, to deal with the issue of updating SaaS apps. A framework for API gateways called SecIngress is proposed that as a solution to the problem that it is difficult to update applications that are based on N-variants while operating in a cloud environment. Metadata polling and operation delay reduction had been accomplished via the implementation of a two-stage timeout execution approach.In order to demonstrate the efficacy of SecIngress, we put together a prototype, install it in a testbed environment, and then compare the security and performance metrics obtained before and after the deployment of the prototype.

Novkovic et al., 2021 [21] addressed the risks of information leaks and repudiate faced by cloud service companies and the steps taken to lessen or eliminate those risks. Researchers zeroed in on the cloud's internal workings, and the source of the risks, and proposed a way to protect user privacy while reducing those dangers. The purpose is to equip service providers operating in cloud-based settings with a better understanding

Kandoussi et al., 2020 [22] suggested a"honeypot and virtual machine migration" as potential components of a cyber-security protection model. Through the implementation of privacy regulations, the suggested architecture is resilient to assault, and it can also categorize cyber-attacks into two groups. In this study, a unified defensive architecture that utilizes both honeypots and movable virtual machines. Security policy considerations are utilized to estimate the efficacy of the suggested system. As a result, the attack graph is integrated with stochastic game theory to explain the attacker-defender interaction. We conclude with some statistical results that show how well the suggested security game model works.

Chalkiadakis et al., 2020 [23] presented a solution for wireless carriers to establish a realistic authentication that facilitates the delivery of a single, uninterrupted operation to end users of cloud-hosted applications. They also employed a buffering technique to try to eliminate the delays that result from constantly transmitting and obtaining information from faraway places. When contrasted to traditional TLS handshakes, the results from this method are more favorable.In this work, develop and build a functional attestation system that makes it possible for a service provider to provide an attestation service that is seamless between hosted apps and the end users of such applications. In addition, we reduce the latencies caused by the remote attestation process by implementing a unique caching system that is capable of doing so. The solution makes it possible for the parties to authenticate one another before to each attempt at communication, and these results in enhanced performance in comparison to a traditional TLS handshake.

Koo et al., 2019 [24] discussed issues of safety in cloud applications. Investigators said that the community security information platform's current privacy infrastructure is inadequate. To construct a structure for societal data privacy safety, they developed architecture for encryption that is reliant on networked processing. In order to find a solution to this issue, it will be important to develop the safe security architecture of the national military command control system while taking into consideration the security needs associated with cloud computing. In this paper, the necessary safety precautions for the implementation of cloud computing by the United States military are analyzed. It also evaluates Korea's national military information system's current security demands and cloud computing security requirements to determine cloud-based security requirements.

Raja 2018 [25] suggested a symmetric encoding technique for cloud database privacy using to create a secret key, an alphabetic encrypting matrix is needed. Typically, those credentials are the first line of defense in a user's verification process. The use of various algorithms makes information hacker-proof. When a business makes use of cloud computing, there are a variety of concerns about the safety of their data that arise during the data life cycle, which consists of five stages. It is provided that a data management framework has been handed forth, which not only includes the data categorization but also the risk management framework.

Mosola et al., 2017 [26] developed a technique to lessen cyber assaults on cloud storage facilities dedicated to keeping data secure. Client-side encoding and credential handling is their proposed method for doing this. A new cryptographic technique is derived from the combination of chaos theory and neural encryption. This approach improves the confidentiality of encoded information by concentrating on the unpredictability of the arriving major disruption rather than the length of the encryption. The purpose of this study is to suggest a client-end encryption and

key management system as a means of preventing cyberattacks whose primary objective is to violate the confidentiality of data stored in the cloud.

Timothy and Santra 2017 [27] advocated for a paradigm that combines several cryptographic techniques, such as Blowfish, RSA, and SHA-2. This method is a combination of symmetrical and asymmetrical approaches. The Blowfish strategy ensures data privacy, while the RSA method verifies identities, and the SHA2 mechanism checks for information corruption. This scheme offers robust protection for sensitive information sent over the World Wide Web.The purpose of this research was to develop a whole new security solution for securing data stored in the cloud by using a hybrid cryptosystem. Encrypting the user data at the time of data transmission is necessary for the ongoing inquiry since it is necessary to safeguard data in the cloud from unauthorized access or hackers at the time of data transmission.The current research came to the conclusion that the suggested technique offers a high level of security for the transmission of data over the internet as well as appropriate network access on demand to a pool of shared computing resources that are primarily composed of a storage usage, a server, and the internet.

Alshammari et al., 2017 [28] explored "distributed computing" in aspects of dispersed computing, lattice registration, and virtualization operation; evaluated and talked regarding privacy attacks and possible configurations, and checked the health of the "distributed computing" environment. Cloud computing has developed into a potentially lucrative business idea for the computing infrastructure industry, which is seeing a rise in the number of worries over the level of security provided by an environment. In the context of cloud computing, one of the most pressing concerns is data protection and safety. In this work, analyze some of the most prominent security threats to clouds and some potential responses to those threats: Attacks Using XML Signature Wrapping, Concerns Over Browser Security, and the Problem of Vendor Lock-in.

Salah et al., 2017 [29] suggested a conventional approach that may be used to examine database operation in networking and record their behavior. The hypo-exponential suggested approach was implemented using queueing frameworks, and its functionality was evaluated using a variety of metrics, including transmission errors, latency, queue length, network usage, etc.The purpose is to suggest an analytical model that can capture the behavior of network servers or other systems that behave in a similar manner and then examine that behavior's performance. And able to obtain important performance characteristics and measurements using our model. These characteristics and measures include CPU use, system idleness, mean productivity, packet loss, mean systems and queued packet delays, and mean system and queue sizes. The findings indicate that both of these approximation models provide outcomes that are comparable when the queue size of the system is big.

Song et al., 2016 [30] have solved the problems with cloud computing's lack of trust ability and authentication. “Ubuntu Enterprise Cloud" (UEC) has been presented as a means to address virtualized computing's authentication and access concerns. This method does this via the use of encrypted and decrypted data. UEC makes sure that even when admins need accessibility to the entirety of a client's information to do their jobs, they don't receive carte blanche. It keeps users' information private by checking that the cloud's design shields it from prying eyes. The electronic voucher may be exchanged in person for the corresponding retail item at the physical location that represents the online social network. In this case, a display is made up of both thedigital image and electronic voucher.

Suryawanshi and Shelke 2016 [31] address data accessibility, the authenticity of the information, and information protection by presenting two methods. Their first plan is to monitor the audience. As the scheme's Third Party Authenticator, the Homomorphic Linear Authenticator is used. Threshold cryptography is their alternative plan B. The first method guarantees that TPA will learn nothing crucial during the auditing process, while the second guarantees that the information will remain safe from prying eyes. Also suggested a new framework that is based on hybrid encryption schemes in order to tackle the problem of data security in cloud computing. This framework is able to encrypt data as well as recover it in an effective manner. The performance assessment and validation of the suggested model has been carried out, and the results of the performance analysis have indicated that our design is viable, scalable, and effective.

Negi et al., 2015 [32] introduced a paradigm where counter-propagation neural networks are used for both encrypting and decoding. It improves upon the standard safety measures. There is talk of a three-tiered authenticating system that may strengthen data protection. The play itself is not discussed. In addition to ensuring that the forensic virtualized environment is running properly, the suggested approach also includes real-time surveillance of the network.For cloud service customers' data security, the Framework emphasizes encryption and decryption. Performance is not addressed by the proposed solution, which only improves safety. A forensic virtual machine, malware detection, and system monitoring are all part of the package. In addition, this article covers many information security weaknesses and threats. Cloud service providers and customers should have transparency in a data security framework to mitigate data security risks.

Khan and Tuteja 2015 [33] presented a multi-stage encryption/decryption scheme to enhance cloud safety. If a hacker or other unauthorized user were to employ this method, they would be required to decode the information at each level, which is significantly more difficult than decoding entire information at a single level. The strategies used at each of the three stages are the "Data Encryption Standard" (DES), the "Advanced Encryption Standard" (AES), and the "Rivest-Shamir Adleman" (RSA). Its purpose is to prevent unauthorized individuals from gaining access to the information.Computing in the cloud refers to an internet-based advancement that is used in computer technology. Data

privacy, security, anonymity, and dependability are just few of the issues that often arise in conjunction with cloud computing. However, the most significant aspect of each of them is the cloud provider's security measures and how they are implemented. When we talk about securing the Cloud, we are referring to securing both the treatments (calculations) and the storage (databases housed by the Cloud provider). In this research, investigated a variety of cloud-related security flaws in addition to a variety of cryptographic protocols that may be used to improve cloud safety.

Table 1 illustrates a comparative study of literature reviewed during the investigation of finding the cloud security-enhancing techniques and algorithms.

Table 1. A comparative study of literature reviewed during the investigation

Author, Year	Objectives	Techniques	Results
ThandaiahPrabu et al., 2022 [19]	In this research, the author provides a unique Multi-Data Management Cipher Strategy for employment in creating indexes and formulating inquiries.	Trusted cluster method with depth-first searching	The capacity of the suggested method to preserve data securely in a cloud setting is shown, both in theory and in visual form, by the method itself and by the examples provided.
Zhou et al., 2021 [20]	to address the difficulty of working in the cloud, SecIngress is proposed as an API gateway architecture.	The method with N variations, Voting using Analytic Hierarchy Model	SecIngress improves cloud operations' dependability with a tolerable impact on execution, according to the study's findings.
Novkovic et al., 2021 [21]	to offer light on the difficulties network operators have in cloud-based systems in avoiding data theft and data integrity concerns	provider of safe services, private online transactions	Learn more about sensitive computing to protect sensitive information and lessen the likelihood of a data breach occurring inside your organization.
Kandoussi et al., 2020 [22]	create a hybrid security architecture by integrating VM migration and honeypot	Virtual machine migration with honeypots	The outcomes prove the viability of the suggested security game concept.
Chalkiadakis et al., 2020 [23]	Create an efficient mechanism for attesting services so that providers may give their clients a streamlined experience.	MRSIGNER, SGX, ISV, TCB, SVN	Better functioning is seen when contrasted to a regular TLS handshake.
Koo et al., 2019 [24]	Determine what precautions should be taken to ensure the cloud computing infrastructure is secure.	the technology used in the cloud, security architecture for C4I operations in the cloud	evaluate the current state of database infrastructure security in Korea's military
Raja 2018 [25]	to createan effective data backup system and put that system for faster decoding and encoding processes.	EDSMCCE	The findings prove that the information is kept in a safe location where neither administrators nor others may have access to it.
Mosola et al., 2017 [26]	client-side encrypting and credential governance to prevent cyberattacks on cloud storage systems' security	Digital Equipment Security, Three-Circuit Cryptography, Cryptor, Neural Network	When comparing encoding and decoding times, the results show that Cryptor is the superior method.
Timothy and Santra 2017 [27]	creating a novel approach to security for cloud-based data storage by utilizing a modified cryptosystem	RSA (asymmetric) and Blowfish (symmetric)	The suggested technique ensures safe worldwide web information transfer and instantaneous, appropriate network connectivity.
Alshammari et al., 2017 [28]	studying prevalent cloud privacy threats and potential countermeasures	XML, REST,	found the problems, analyzed them, and picked the optimal remedy out of the options available.
Salah et al., 2017 [29]	provides a quantitative framework for observing and assessing server activity in a network	M/D/1/K model, M/M/1/K model	Whenever the queue size of the network is big, studies demonstrate that both approximation approaches perform similarly.
Suryawanshi and Shelke 2016 [31]	presents two strategies for protecting cloud-based information	Linear holomorphic authenticators and threshold cryptography	The first approach prevents the TPA from any information.the second method ensures that cloud-based data is safe.
Negi et al., 2015 [32]	emphasizes the encoding and decoding process to provide the safety of their data	MD5, RSA, PDP, PoR, neural cryptography.	information protection risks in cloud environments may be mitigated thanks in part to the clarity provided by the architecture.

3. Methodology

We proposed encrypting user-provided data using only the P-AES technique for material with a typical level of privacy concern. We proposed the random forest for classifying the information thenwe devised the RC6 technique for encryptiondata and encrypting its key using the 3DES technique. The MD5 hashing technique is used to create a hash value, which is then stored as a numerical value when each encoded document is created. Afterward, the generated hash value and encoded confidential key are sent to the internet. The platform will verify the hash number to see whether it is identical after it receives the signed message and RC6 encrypted secret key and uses its private key and 3DES to decode

the encrypted secret key to obtain the initial private key. If they match, the communication will be saved in the cloud; else, it will be deleted and then the additional response will be delivered to the client to explain that the communication was not secured and might have been changed in transit. Having this data at hand will allow the user to send identical communication again. By doing this, we produced an algorithm that provides the document's privacy, authenticity, and delivery to the intended recipient, and the Pseudo code for sensitive data encryption is shown in Table 2.

Table 2. Pseudocode for sensitive data encryption

"RC6 Encryption
Input: Raw data S_{ia} stored in four w-bit input registers A, B, C, D.
Number of Rounds: K
W-bit round Keys S[0, …….., 2R+3]
Output; Ciphertext of given data stored in A, B, C, D.
Procedure
//Prewhitening
B=B+S[0]
D=D+S[1]
//Inner Loop Rounds
For i=1 to K do
{
T=(Bx(2B+1))<<$\log_2$w)
U=(Dx(2D+1))<<$\log_2$w)
A=((A t)<<u)+S[2i]
C=((C u)<<t)+S[2i+1]
(A,B,C,D)=(B,C,D,A)
}
//Postwhitening
A=A+S[2r+2]
C=C+S[2r+3]
Fiestel Encryption
Input: Raw data S_{ib} given as input to the Fiestel
Round Function: F and 'r'rounds
Round Keys: K_0…….K_n
Output: Cipher data of given input
Procedure"
//Data splitting
$S_{ib}=S_{ibL} + S_{ibR}$
Compute S_{ibL} (r=1) and S_{ibR} (r=1) functions
Cipher data → S_{ibL+1} andS_{ibR+1}

3.1 Techniques

- **RC6**

The standard implementation of RC6 has a block size of 128 bits and offers key sizes of 128, 192, and 256 bits respectively. The construction of RC6 is extremely similar to that of RC5, using data-dependent rotations as well as modular addition and XOR operations. In point of fact, RC6 may be seen as the interlacing of two separate RC5 encryption procedures at the same time. However, RC6 makes use of an extra multiplication operation that RC5 does not have. This is done so that the rotation is dependent on each and every bit that makes up a word, rather than only the few bits that are considered to be the least critical. This particular procedure is not a part of the RC5 protocol [34].Fig 1illustrate the block diagram of RC6 encryption as shown below.

- **3DES**

The standard DES algorithm had a number of flaws that needed to be addressed, and the development of Triple DES was undertaken to address these issues. The only difference between DES and Triple DES is that the DES algorithm is employed three times in Triple DES rather than only once. The 3DES algorithm may utilize either two or three keys, depending on the size of the key that is needed; for example, using two keys provides a key size of 112 bits, while using three keys provides a key size of 168 bits [35].Documents can be shared and collaborated on in a group setting as Fig 2 shows the 3DES encryption and Decryption flowchart.

3DES with two keys

When we encrypt data using DES with two keys, for example k1 and k2, we have to choose between those keys twice throughout the procedure. First, we will cipher plain text using key k1, then we will decode the previously encrypted text using key k2, and lastly, we will cipher the previous result using key k1.The algorithm is the same as the one used by DES. In this case, we employ two different keys, each of which is 56 bits, giving us a total key size of 112 bits. By setting k1=k2, this method may be used in place of a conventional DES.After then, the procedure will be something along the lines of first encrypting the plain text with key k1, then decrypting the cipher text with key k2 (which is really key k1), which means that we will now have plain text once again, and now we will encrypt the plain text with key k1 [36].

3DES with three keys

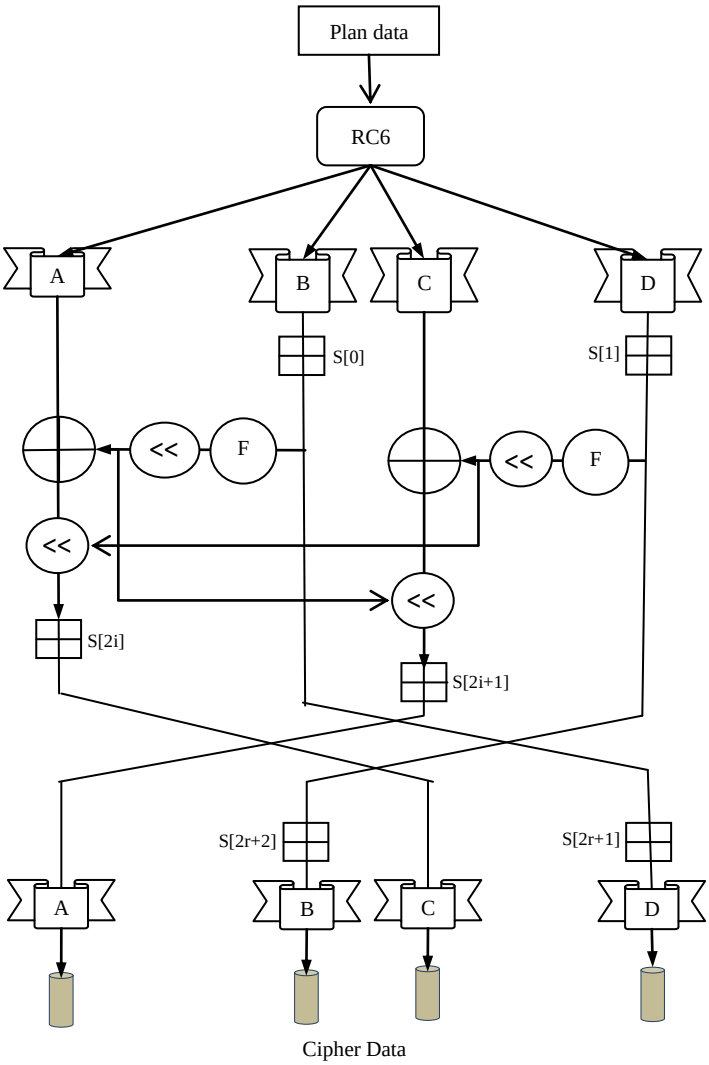


Fig. 1. RC6 encryption flow chart [15]

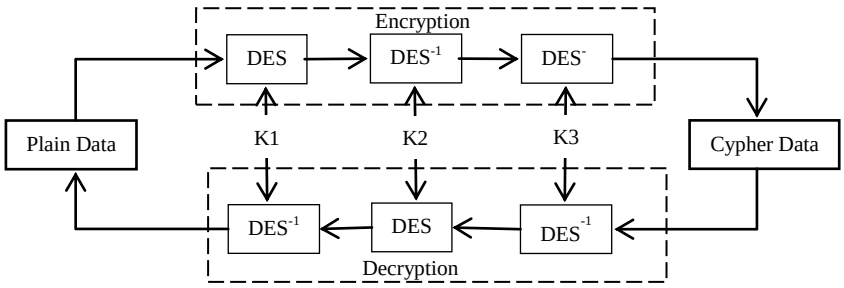


Fig. 2. 3DES encryption and decryption flowchart [10].

This particular technique makes use of three keys, which results in a key size of 168 bits. This results in an increased degree of security for the algorithm. It is distinct from two key-3DES due to the fact that here, we do not employ the first key at the very end again; rather, we use the third key (k3) for the very last encryption. Its keys have a size that corresponds to the number of keys used in the method, which is 112,168 bits, making it more secure than the traditional version of DES.Due to the large size of the key space in 3DES, exhaustive search is unable to decrypt the key. As a result of the fact that 3DES employs three keys, it is easy to see why its processing time is three times as long as that of DES [36].

3.2 Tool

The experiment analysis was carried out in Python. The proposed framework is implemented on different file sizes. The hybrid algorithm will provide the security of data. Message Digest as a digital signature will provide authenticity.

With the suggested paradigm, information is encrypted using the RC6 method before being sent to the cloud, and the key for that process is encrypted using the 3DES technique. Whenever a client wishes to share a document, they must initially submit that to the cloud database, where the RC6 method and the utilized 3DES technique are employed for encrypting. The following explains how the recommended approach works.

Sender: Encryption

- The user places the informational document in cloud services.
- As the primary layer of cryptography, 3DES is used, and as the second, RC6 is used.
- Finally, the data is converted into the Cipher Text, which is stored in the database.

3.3 Dataset

The dataset used in this research is generated by the piidetect python library and the link to this library is "https://pypi.org/project/piidetect/". This library generated multiple person personal information like address, card number, phone number, bank account number, etc. we categorized this information into normal and highly sensitive information

4. Result and Discussion

The experiments are conducted on a range of different sizes using RC6 and 3DES as the algorithms. The efficiency, as well as other metrics, are included into the overall evaluation of these algorithms together with criteria such as the amount of time needed for their execution and the amount of related memory. Discovering which of the previously outlined methods of encryption is both the quickest and most secure is the objective of the approach that has been recommended. Therefore, it gives the user the ability to modify the encryption algorithm to one that is more suitable for the material that they wish to encrypt. The findings indicate that the suggested approaches boost the efficiency of encryption algorithms by encrypting data safely in a shorter period of time.Concerns about data security have been the biggest roadblock to the wider use of Cloud services. Numerous people may feel uneasy about entrusting their data and programs to another person's hard drive and computer processor.Loss of data, scamming, and botnets (a network of computers controlled externally) are all well-known security problems that pose major risks to an institution's documents and software. Furthermore, the multi-tenancy architecture and shared computing resources of cloud computing introduce new security concerns that need novel solutions.

Fig 3 demonstrate that the code running in colab as shown below. We develop an algorithm using 3DES and RC6 encryption to secure the cloud data to deal with these security issues. The developed algorithm codes are written in python language and run in Google's Colab simulator utilityto execute the developed algorithm as shown below. An encoding technique was only performed on the data that was transmitted into this system.The functionality of the platform is evaluated by uploading encrypted files of varying sizes that are kept in the cloud storage space. The data will be encrypted cost-effectively and safely using the suggested approach. The size of the file might vary anywhere from 10 KB to 1000 KB at most.

Fig. 3.Code running in Colab

Fig4 depicts the 2x2 confusion matrix andthe analysis of the confusion matrix depicts that the proposed encryption method canencrypt the data with less investment cost.This matrix is discussed in terms of both the value that it really has and the value that it is expected to possess. In order to present a clear and simple breakdown of the total number of correct and faulty forecasts, count values are used. The number 1614, which stands for the true positives, is represented by the symbol Tp, whereas the number 9, which stands for the false positives, is represented by the symbol fp. The notation fn = 424 is used when referring to a false negative, whereas the notation san 1 is utilized when referring to a genuine negative.

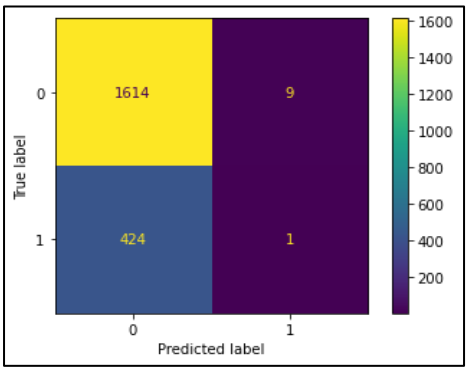
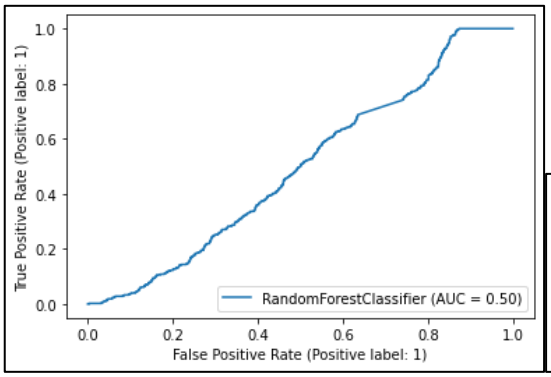


Fig. 4. Confusion matrix

Fig 5 (a) and (b) illustrate the receiver operating characteristic curve between true positive value and false positive values and the classification report corresponding generated while encrypting the cloud uploaded data using the proposed encryption algorithm. Fig 5 (b) indicate an analysis of the receiver operating characteristic curve and classification report depicts that the proposed encryption method is sufficiently able to encrypt the sensitive information present in the uploaded data within less encryptiontime. There are some parameter has examined such as precision, recall, f1-score which determined in terms of normal and high. The normal precision is 0.79, and high precision is 0.10, normal recall is 0.99, while normal f1-score is 0.88 as shown below.



(a)

	precision	recall	f1-score	support
Normal	0.79	0.99	0.88	1623
High	0.10	0.00	0.00	425
accuracy			0.79	2048
macro avg	0.45	0.50	0.44	2048
weighted avg	0.65	0.79	0.70	2048

(b)

Fig. 5. (a) receiver operating characteristic curve (b) classification report

Fig 6 and 7 depict the comparison of Amazon EC2 based on rejection time and P-value. For a clearer picture of the outcomes, we evaluated the proposed encoding technique with 8 existing encoding techniques based on P-value and rejection rate, with a greater P-value indicating a superior technique and the opposite being true for a larger rejection rate [37]. From the Fig 6, it is clear that the suggested technique beats all the techniques in the Amazon EC2 based on rejection rate and P value respectively, indicating that the proposed algorithm outperforms the standard encryption algorithms such as AES, 3DES, blowfish, two-fish, MARS, DES, RC4, and RC6 in terms of encryption rejection rate and P-value.From the Fig 7, it is clear that the proposed method attained high amazon EC2 based on P-value as compared to other methods while RC6 algorithm obtained low amazon EC2 based on p-value as shown below. Thus, from the present work we can say that with the integration of 3DES encryption and RC6 encryption algorithms in the proposed work, a strong encryption infrastructure could be made to enhance the security of cloud computing data. The investigation shows that when it comes to Amazon Elastic Compute Cloud (EC2), most users recommend the AES technique for the highest level of confidentiality [38], while those who prioritize speed of information acquisition opt for Blowfish's DES [38]. However, a combination technique combining AES, RC6, and 3DES provide asuperior level of protection in a fraction of the time. The suggested approach is contrasted with the AES, Blowfish, TwoFish, RC6, MARS, DES, RC4, and 3DES techniques to provide a level of information confidentiality on a block-by-block basis.

We present a method that combines elements of the AES, RC6, and 3DES encryption techniques in our proposed work. Symmetric key encryption describes all techniques for encrypting the files, these techniques only need one key.

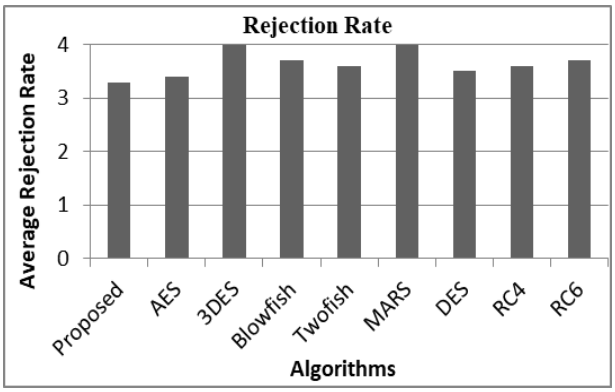


Fig. 6. Comparison of Amazon EC2 based on rejectionrate

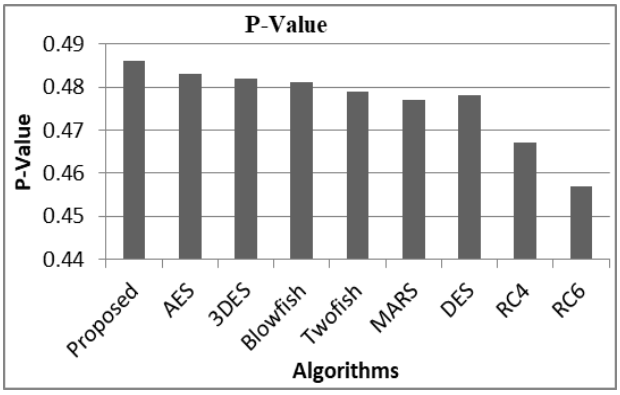


Fig. 7. Comparison of Amazon EC2 based on P-Value

Fig 8 illustrates the comparison of encryption time as shown below. The proposed method is compared to other methods with different file size. The blowfish method takes the following file sizes into consideration when calculating the encoding time: 100 KB, 200 KB, 400 KB, and 800 KB. The encoding time is measured in seconds. In all techniques, the key size is 128 bits. Python is used to develop the actual workings of the suggested framework. Python code is used to determine the length of time required for encrypting a document. The time needed to encrypt a document file is determined by comparing the various encoding techniques currently in use. The duration of time needed for encryption is shown clearly in Fig 8. From the Fig 8, it is clear that the 100KB file size attained high encryption time while proposed method achieved less encryption time for 100KB file size. The proposed method is attained less encryption time in different file size as compared to other technique. When 3DES is used for encryption, AES is used for substitution, and RC6, AES, and the 3DES algorithm are all used for key generation, security is increased while overall time is reduced compared to using the aggregation method. Variability in the data uploading technique is represented by the size of the data in bytes.

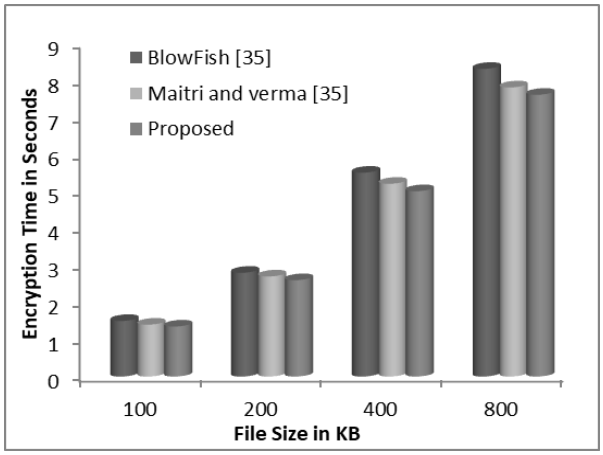


Fig. 8. Encryption Time Comparison with Proposed System [35]

5. Conclusion and Future Scope

The safety of cloud data and users is becoming more important as the popularity of cloud computing soars. Multiple approaches to cloud security are possible. Data storage on the cloud is becoming more common, yet privacy remains a major concern for businesses. In this study, we constructed the encryption algorithms 3DES and RC6 to fortify cloud computing against potential threats. Therefore, we presented a multilayer encoding cryptographic technique to add another level of protection to data transfers between the user and the cloud platform. According to the analysis, which included the performance of the method, the recommended technique is more effective than the current approach. This new method is presented to increase the security of encrypting credentials by using unpredictable randomized disturbance. In comparison to previous technique, the methodology accomplishes encryption in a small amount of time. According to the findings, the proposed method gives outperformance and attained less encryption time in different file size as compared to other methods. Therefore, the proposed algorithmic system is useful for present-day needs. To prove the effectiveness of the proposed architecture, it may be necessary to conduct future comparisons with alternative cloud security methods. Therefore, there will be increased efforts to reduce encryption delays. In the long term, this approach may be integrated with AI methods to significantly improve cloud infrastructure privacy. To further strengthen encryption and cloud security, new algorithms should be developed from current ones.

References

[1] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, “A comparative study of class rebalancing methods for security bug report classification,” IEEE Transactions on Reliability, vol. 70, no. 4, pp. 1658–1670, 2021.

[2] Z. Lv, L. Qiao, and I. You, “6G-enabled network in box for internet of connected vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5275–5282, 2021.

[3] R. Liu, X. Wang, H. Lu et al., “SCCGAN: style and characters in painting based on CGAN,” Mobile Networks and Applications, vol. 26, pp. 3–12, 2021.

[4] B. Cao, Y. Gu, Z. Lv, S. Yang, J. Zhao, and Y. Li, “RFID reader anticollision based on distributed parallel particle swarm optimization,” IEEE Internet of 9ings Journal, vol. 8, no. 5, pp. 3099–3107, 2021

[5] H. Cheng, M. Shojafar, M. Alazab, R. Tafazolli, and Y. Liu, “PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, 2021.

[6] Z. Lv, D. Chen, H. Feng, H. Zhu, and H. Lv, “Digital twins in unmanned aerial vehicles for rapid medical resource delivery in epidemics,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–9, 2021.

[7] B. Cao, S. Fan, J. Zhao et al., “Large-scale many-objective deployment optimization of edge servers,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3841–3849, 2021.

[8] H. Chen, Y. Xiong, S. Li, Z. Song, Z. Hu, and F. Liu, “MultiSensor data driven with PARAFAC-IPSO-PNN for identification of mechanical nonstationary multi-fault mode,” Machines, vol. 10, no. 2, p. 155, 2022.

[9] Z. Lv, Y. Li, H. Feng, and H. Lv, “Deep learning for security in digital twins of cooperative intelligent transportation systems,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2021.

[10] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[11] B. Cao, Z. Sun, J. Zhang, and Yu Gu, “Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3832–3840, 2021.

[12] J. Chen, Y. Liu, Y. Xiang, and K. Sood, “RPPTD: robust privacy-preserving truth discovery scheme,” IEEE Systems Journal, pp. 1–8, 2021.

[13] T. Cai, D. Yu, H. Liu, and F. Gao, “Computational analysis of variational inequalities using mean extra-gradient approach,” Mathematics, vol. 10, p. 2318, 2022.

[14] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, “Improving high-impact bug report prediction with combination of interactive machine learning and active learning,” Information and Software Technology, vol. 133, Article ID 106530, 2021.

[15] Atiewi, Saleh, Amer Al-Rahayfeh, MuderAlmiani, Salman Yussof, Omar Alfandi, AhedAbugabah, and YaserJararweh. "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography." IEEE Access 8 (2020): 113498-113511.

[16] Z. Niu, B. Zhang, B. Dai et al., “220 GHz multi circuit integrated front end based on solid-state circuits for high speed communication system,” Chinese Journal of Electronics, vol. 31, no. 3, pp. 569–580, 2022.

[17] F. Zhao, L. Song, Z. Peng et al., “Night-time light remote sensing mapping: construction and analysis of ethnic minority development index,” Remote Sensing, vol. 13, no. 11, p. 2129, 2021.

[18] H. Wang, Q. Gao, H. Li, H. Wang, L. Yan, and G. Liu, “A structural evolution-based anomaly detection method for generalized evolving social networks,” 9e Computer Journal, vol. 65, no. 5, pp. 1189–1199, 2022.

[19] ThandaiahPrabu, R., P. Vijayakumari, K. Chanthirasekaran, K. Jayamani, and P. Nirmala. "An Efficient and Secured Multiple Keyword Cloud Data Searching Scheme with Dynamic Encryption Procedure." In 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp. 1-6. IEEE, 2022.

[20] D. Zhou, H. Chen, G. Cheng, W. He, and L. Li, “SecIngress: an API gateway framework to secure cloud applications based on N-variant system,” China Communications, vol. 18, no. 8, pp. 17–34, 2021.

[21] B. Novkovic, A. Bo ´ zi ˇ c, M. Golub, and S. Gro ´ ˇs, “Confidential computing as an attempt to secure service provider’s confidential client data in a multi-tenant cloud environment,” in Proceedings of the 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 1213–1218, IEEE, Opatija, Croatia, September 2021.

[22] E. M. Kandoussi, M. Hanini, I. El Mir, and A. Haqiq, “Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game,” Telecommunication Systems, vol. 73, no. 3, pp. 397–417, 2020.

[23] N. Chalkiadakis, D. Deyannis, D. Karnikis, G. Vasiliadis, and S. Ioannidis, “)e million dollar handshake: secure and attested communications in the cloud,” in Proceedings of the 2020 IEEE 13th International Conference on Cloud Computing (CLOUD), pp. 63–70, IEEE, Beijing, China, October 2020.
[24] J. Koo, Y.-G. Kim, and S.-H. Lee, “Security requirements for cloud-based C4I security architecture,” in Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), pp. 1–4, IEEE, Jeju, Korea, January 2019.
[25] Raja, K. "Enhanced Data Security Methodology for Cloud Computing Environment." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3 | Issue 3 | ISSN: 2456-3307 (2018).
[26] Mosola, N. N., M. T. Dlamini, J. M. Blackledge, J. H. P. Eloff, and H. S. Venter. "Chaos-based Encryption Keys and Neural Key-store for Cloudhosted Data Confidentiality." (2017).
[27] Timothy, Divya Prathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." In 2017 International conference on microelectronic devices, circuits and systems (ICMDCS), pp. 1-5. IEEE, 2017.
[28] A. Alshammari, S. Alhaidari, A. Ali, and Z. Mohamed, “Security threats and challenges in cloud computing,” in Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 46–51, IEEE, New York, NY, USA, June 2017.
[29] K. Salah and S. El Kafhali, “Performance modeling and analysis of hypoexponential network servers,” Telecommunication Systems, vol. 65, no. 4, pp. 717–728, 2017.
[30] Song, Tailim,Dae young and Jim chul Kim, “Device,system and method of enhancing user privacy and security within a location-based virtual social networking context." U.S. Patent 9,245,282, issued January 26, 2016.
[31] Suryawanshi, Reshma, and Santosh Shelke. "Improving data storage security in cloud environment using public auditing and threshold cryptography scheme." In 2016 International Conference on Computing Communication Control and automation (ICCUBEA), pp. 1-6. IEEE, 2016.
[32] Negi, Anshika, Mayank Singh, and Sanjeev Kumar. "An efficent security farmework design for cloud computing using artificial neural networks." International Journal of Computer Applications 129, no. 4 (2015): 17-21.
[33] Khan, Shakeeba S., and R. R. Tuteja. "Security in cloud computing using cryptographic algorithms." International Journal of Innovative Research in Computer and Communication Engineering 3, no. 1 (2015): 148-155.
[34] Mathur, Milind, and Ayush Kesarwani. "Comparison between des, 3des, rc2, rc6, blowfish and aes." In Proceedings of National Conference on New Horizons in IT-NCNHIT, vol. 3, pp. 143-148. 2013.
[35] Singh, Sombir, Sunil K. Maakar, and Dr Sudesh Kumar. "Enhancing the security of DES algorithm using transposition cryptography techniques." International Journal of Advanced Research in Computer Science and Software Engineering 3, no. 6 (2013): 464-471.
[36] Singh, Mandeep, and Narula Simarpreet Singh. "Implementation of Triple Data Encryption Standard using Verilog." International Journal of Advanced Research in Computer Science and Software Engineering 4, no. 1 (2014).
[37] Mohamed, Eman M., Sherif El-Etriby, and Hatem S. Abdul-kader. "Randomness testing of modern encryption techniques in cloud environment." In 2012 8th International Conference on Informatics and Systems (INFOS), pp. CC-1. IEEE, 2012.
[38] Maitri, Punam V., and Aruna Verma. "Secure file storage in cloud computing using hybrid cryptography algorithm." In 2016 international conference on wireless communications, signal processing and networking (WiSPNET), pp. 1635-1638. IEEE, 2016.

Authors’ Profiles

Chandra Shekhar Tiwari is a Research scholar in the department of Computer, Science and Engineering, Birla institute of technology Mesra, Ranchi, India.

He has completed his Bachelor Degree from RGPV University Bhopal, Madhya Pradesh and Master Degree from RGPV University, Bhopal(MP), His current research interest includes Big Data Analytic, Cloud Computing security, Machine Learning and network security.

Vijay Kumar Jha is working as an Associate Professor in the Department of Information Technology, Birla institute of technology Mesra, Ranchi. He has completed BE (Electronics) from SIT Tumkur in 1996, M.Sc. Engineering in Electronics from MIT Muzaffarpur in 2007 and PhD in Information Technology (Data Mining) from MIT Muzaffarpur in 2011. He has been associated with Birla Institute of Technology, Mesra, Ranchi since 2001. His research interests include Big data Analysis, Data mining, Network Security, ERP etc.

How to cite this paper: Chandra Shekhar Tiwari, Vijay Kumar Jha, "Enhancing the Cloud Security through RC6 and 3DES Algorithms while Achieving Low-Cost Encryption", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.5, pp. 48-59, 2023. DOI:10.5815/ijwmt.2023.05.05