Enhancing Cloud Security: A Hybrid Cryptographic Approach Combining AES and RSA for Optimal Data Protection

Sonia Chamoli [1], Zakir Hussain [2]

[1] Assistant professor, DAV Centenary College Faridabad

[2] Assistant Professor DAV Centenary College Faridabad

ABSTARCT: *As technology develops, the cloud is turning into a repository for private information, making it increasingly vulnerable, especially as more people with bad motives get a hold of it. Data needs to be secure and safe because so many people use the cloud for various reasons. A new hybrid encryption process that combines symmetric and asymmetric cryptographic techniques to create a safe environment is proposed in this paper, which analyzes the well-known symmetric Advanced Encryption Standard (AES) method and the asymmetric Rivest-Shamir-Adleman (RSA) method based on time complexity, space, resource, and power consumption. Based on experimental research, this report recommends that the RSA3DSA and DES cryptographic methods be used as the main strategy for data encryption activities in cloud applications.*

Keywords: Cloud Computing, Security, Cryptography, RSA.

I.INTRODUCTION

The rapid progress in technology is accompanied by daily advancements in technology. Cloud computing presents a novel approach to service delivery by reorganizing several sources and rendering them available to customers only upon their request [1]. The cloud operates similarly to a software program that has been virtualized. Additionally, it is essential to the future technologies of cellular networks & services. Since it significantly reduces customers' storage costs and provides them with convenience, data stored in the cloud has emerged as one of the most significant cloud services. With cloud computing, a person or organization can access a service online without needing to set it up on their own computer.

The low prices, increased storage capacity, & flexibility of cloud computing are its primary advantages. The largest challenge to cloud computing is security and privacy, which is recognized as a serious problem that impacts the system's functionality (i.e., by using the practice of keeping sensitive data on someone else's server at an undiscovered place). The architecture and protocols required to protect cloud computing services from cyber attacks are included in cloud safety [2]. Because of this, cloud computing makes extensive use of encryption to guarantee data security, privacy, and compliance. But the existing options are unworkable due to their flaws and inefficiency. When encrypted data is housed inside cloud infrastructure, auditing control of information becomes more challenging, even though the possibility of privacy leaks is significantly reduced. The purpose of this particular challenge is to convene academics and industry professionals to talk about different facets of cloud computing information security and cryptography.

Cloud Computing: Cloud computing is commonly described in two ways [3]. based on the deployment strategy or the cloud service being offered. We can group cloud computing into the following categories using a deployment approach:

Public Cloud : The cloud is free to use for anyone with an internet connection, and they may opt to pay based on how much they use. The files are being hosted by a third party. A few instances are sales force, Windows Azure Service Platform, and Amazon.

Community Cloud: Several enterprises with similar cloud requirements will use a community cloud.

A hybrid cloud is created by combining two or more clouds—public, private, and communal.

We can talk about either of the following, depending on the service that the cloud model offers:

- Infrastructure-as-a-Service, or IaaS
- Platform-as-a-Service, or PaaS
- Software as a Service, or SaaS
- or Testing-as-a-service, Integration, Security, Management, Data, Process, Application, Storage, and Database

The structure of the paper is as obeys. Section II provides a explanation of cryptography. Section III shows the literature survey; Section IV explained the suggested methodology, including a detailed overview of the dataset, metrics, and sequence of steps undertaken during the research experiment. Section V provides the outcomes achieved from the experiment. Finally, Section VI presents the conclusion and outlines potential future research directions.

II. Cryptography

Cryptography is a method of converting data into an incomprehensible form in order to safeguard it from unauthorized parties. The main goal of cryptography is to achieve security in the following three areas: availability, integrity, and secrecy, while also protecting the information from a third party. The privacy of data saved on cloud servers is the main concern of cryptography [3]. Methods can be divided into two categories: (i) symmetric key-based algorithm and (ii) asymmetric key-based computations, often known as public-key sets of principles. Text and media are examples of knowledge that is encoded during transmission and storage in data cryptography to make it incomprehensible, useless, or hidden. Encryption is the term for this processing. Genuine data are extracted from encrypted data via the reverse procedure, called decryption [4]. Although both symmetric and asymmetric keys may be employed to secure data on cloud computing, symmetric key-based methods are quicker than asymmetric keys because of the size of the database itself and the volume of data stored there.

- Asymmetric Algorithms

Using public and private keys, asymmetrical methods are separated into main key or secondary key structures. The private key is kept secret and is employed for decoding, whereas the public key is accessible to all and is used for encoding [5]. Uses of the asymmetric method include Rivest-Shamir-Adleman (RSA), elliptic-curve cryptography, or asymmetric utilities [6].

- Symmetric Algorithms

On the other hand, symmetrical methods use a single private key to both encrypt and decode data [7]. They have the computational capacity to handle enormous volumes of information. Plaintexts, which are blocks of fixed numerals, are encrypted using symmetric techniques. The AES cipher text approach is a more accurate and advanced encryption method.

Given the test results and the text files employed, it has been concluded that the algorithm used by AES performs better than the DES and RSA methods.

Advance Encryption Standard (AES)

Joan Daemen & Vincent Rijmen developed and implemented the Advanced Encryption Standard (AES) method in 2001. It has a block size of 16 bytes (128 bits), variant keys with sizes of 16 (128), 24 (192), and 32 bytes (256 bits), with conversion rounds on a block determined by integer-fixed key sizes. There are ten rounds for the 16-byte key, twelve rounds for the 24-byte key, and fourteen rounds for the 32-byte key. Figure 1 is a diagrammatic explanation of the AES method. After n iterations of application, the final round is distinctive or a round key is appended at the beginning and end of encryption. The reverse process is employed to decrypt.

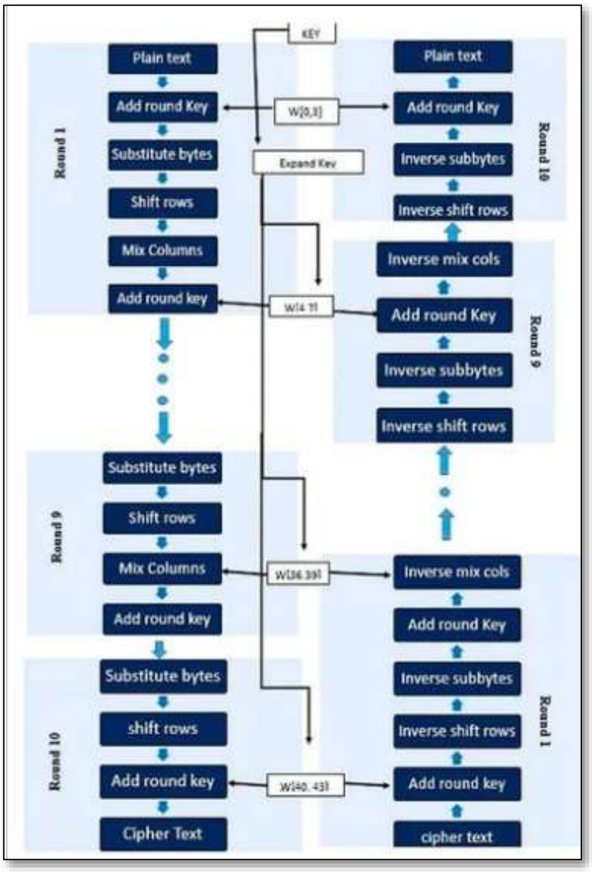


Figure 1. Process of AES algorithm.

AES Merits and De-Merits

Advantages:

Because AES is faster than other computations, it is far more difficult to hack or retrieve the data.

Cons: The software's distribution and execution present a number of difficulties, and complex algebra is overused.

Rivest–Shamir–Adleman (RSA)

RSA is the most used asymmetric or public key cryptography that uses two keys [8]. The sender's public key is used to sign the text, and a secret key is used to decrypt it. This is a versatile, popular method that uses factorizing of primes & accounts for large numbers with primes for security. It is used for maintaining the legitimacy of e-documents, e-commerce safety, public networks, encrypted networks, or emails.

RSA Merits and De-Merits

Benefits: It provides a safe, secure, and encrypted data transport and makes it harder for hackers and crackers to access the content.

A disadvantage is that RSA requires more time, which slows down the process when big amounts of data are used.

III.LITERATURE SURVEY

Praveen et al., (2018) shows how the algorithm known as AES is implemented on an FPGA. FPGA has several benefits, including accuracy, power, portability, speed, and cost. Processing time and device execution were key considerations in the development of the AES algorithm. utilizing a pipeline architecture for the AES technique to boost hardware performance. Operating at 291.68MHz, the proposed sequential AES system can process data at 37.21Gbps. The AES hardware architecture is composed of three mechanisms: FPGA, encryption, and decryption [9].

El_etriby et al., (2012) focused on safeguarding desktop and cloud data storage. They examined eight data encryption methods on personal computers and in a cloud computing environment called Amazon Elastic Compute Cloud (Amazon EC2), like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), Rivest Cipher 4 (RC4), Rivest Cipher (RC6), Two-Fish, Blow-Fish, and MARS. The NIST factual check is used to assess the methods for irrationality as part of the cloud context. A pseudo random number generator (PRNG) is utilized to find the optimal solution [10].

Sengupta et al.,(2015) In order to provide superior cloud data security, a hybrid Rivest Shamir Adleman (RSA) technique has been created. Furthermore, the author concludes that cloud data cannot be adequately protected by a single RSA technique. In order to reduce the possibility of a man-in-the-middle attack, the Feistel Encryption Algorithm is introduced after the RSA encryption technique [11].

Kumar et al., (2021) offered a multilayer cryptography-based cloud computing security plan. The system serves as an example of both symmetric and asymmetric key cryptography methods. By providing several encryption and decryption levels at the transmitter and recipient sides, respectively, the use of the Data Encryption Standard (DES) and RSA in this instance improves the security of cloud storage. This security paradigm encourages clarity for cloud service providers and consumers to reduce security risks. The suggested method was constructed using Java and the cloud simulator program cloud sim. This method increases data safety to the maximum level while speeding up the uploading and downloading of text files compared to the present method [12].

Murali et al.,(2017) The encryption/decryption timings, throughput, and Avalanche impact of a single bit change in the key and plain text in local and cloud contexts are compared using a variety of performance metrics for the 3DES, DES, AES, and Blowfish approaches. The processed data files are between 100 and 600 KB in size. Encryption techniques for simulation results in the cloud environment increase the throughput rate when compared to simulation results in the local environment [13].

Timothy etal., (2017) A new hybrid encryption system is created by combining the Blowfish, RSA, and SHA-2 algorithms. Because the proposed approach makes use of both symmetric and asymmetric algorithms, it works well. The proposed methodology provides good internet data transfer security using the SHA-2 method [14].

Lee et al., (2018) For cloud computing data security, it is recommended to use AES under the Heroku infrastructure. Implementing Heroku as a virtualized environment involves a number of steps. After that, the writers launched a website that serves as a data protection service. AES was used by the authors to secure the site's data. The assessment of performance indicated that AES cryptography might be used for data security. Furthermore, studies of data encryption latency show that higher information delay times are caused by larger data volumes [15].

Amalarethinam et al., (2017) By employing primes instead of arbitrary numbers, the proposed method increases the speed of encryption and decryption. The recommended method, ERSA, increases speed even when the file is divided into numerous parts. The ERSA approach is used to increase speed, but it also increases security and complicates calculation. In the future, the idea of additive chaining could continue to be applied to shorten the encryption and decryption times. To determine the level of security, statistical methods may also be employed to test the procedure's security phase [16].

IV.PROPOSED WORK

- Problem Formulation

Present time is a technology age where different technologies are present in the world. Cloud computing is one of them. It forms an architecture provisioning many it resources as operating systems without direct active management by the user. Infrastructure, software and platform are the services. People store their data on cloud storage very commonly now a day. Security is a major issue in storing data on clouds. Cryptography techniques are very useful to impose security on data. In the existing work a hybrid cryptography system is proposed to provide better security on the data which is stored on cloud storage. The proposed approach use RSA algorithm and DES algorithm and provide a hybrid of the two algorithms to provide more security on the data before storing it on cloud. The proposed algorithm is tested on a sample plain text. As per the literature study DES algorithm less secure .As it became clear that DES did not provide adequate security because of its 56-bit secret key, the cipher was gradually replaced by Triple-DES (also known as TDEA). Once the weaknesses of normal DES became more apparent, 3DES was adopted in a wide range of applications. Although it’s officially known as the Triple Data Encryption Algorithm (3DEA), it is most commonly referred to as 3DES. This is because the 3DES algorithm uses the Data Encryption Standard (DES) cipher three times to encrypt its data.

- Objectives

1. To implement Triple Data Encryption Algorithm (3DEA) for more data security
2. To introduce RSA algorithm based encryption for two-level data security
3. To Performance comparative analysis of proposed work.

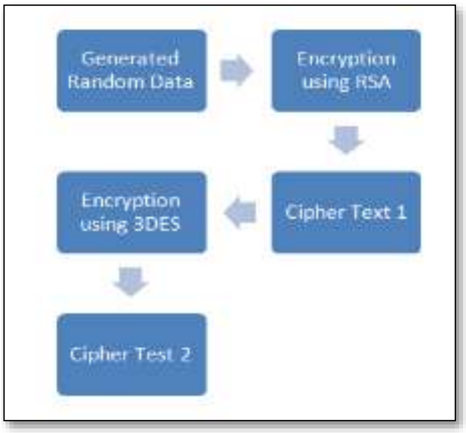
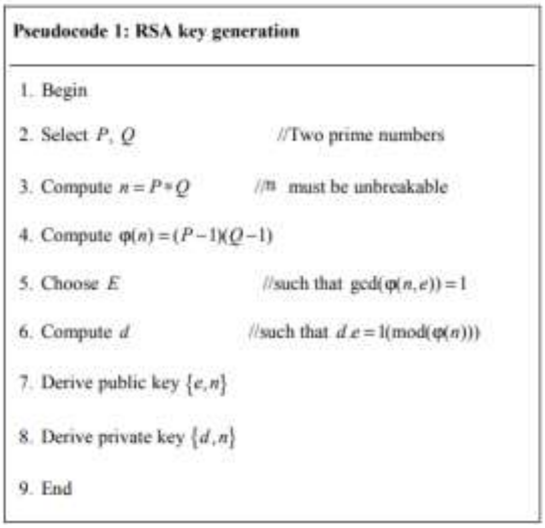


Figure 2: Flowchart of Proposed Work

V.RESULTS

With cloud computing, just the resources used are paid for assaults. Its related to cloud computing include DOS, side-channel, and hypervisor assaults. Client authentication, authorization, hardware virtualization security limitations, flooding attacks, cloud dependability, remote storage security, or outsourcing security assessment are among the security issues associated with cloud computing.

RSA is a well-known asymmetric cryptosystem that encrypts and decrypts data using two different keys. The general RSA key creation process is demonstrated in pseudo code.



```
Pseudocode 1: RSA key generation
1. Begin
2. Select $P$, $Q$                //Two prime numbers
3. Compute $n = P*Q$              //n  must be unbreakable
4. Compute $\varphi(n) = (P-1)(Q-1)$
5. Choose $E$                     //such that $\gcd(\varphi(n, e)) = 1$
6. Compute $d$                    //such that $d.e = 1(\mathrm{mod}(\varphi(n)))$
7. Derive public key $\{e, n\}$
8. Derive private key $\{d, n\}$
9. End
```

These generated keys are used to execute data encryption or decryption. Figure 4.1 shows the RSA algorithm's pipeline layout. The creation of prime numbers is a part of the first step. The key generation process is carried out in the second step. Processes for both decryption and encryption are included in the third step. Data is secured using the RSA method in this way.

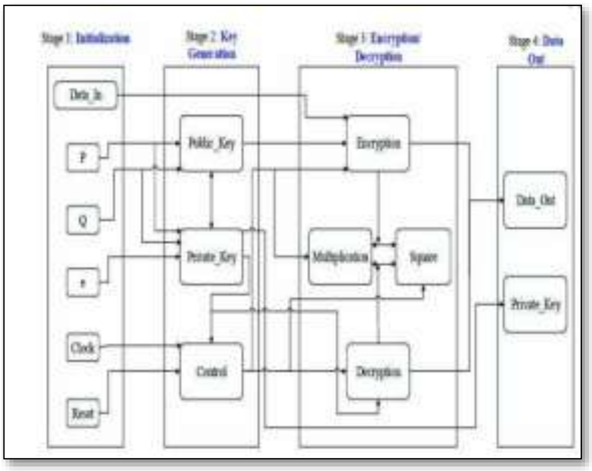


Figure 3; Process in RSA algorithm

The degree of difficulty in factorizing the prime numbers P and Q determines the security grade of the RSA method in the main. Therefore, in order to raise the security level, work has been done to boost the quantity of prime numbers.

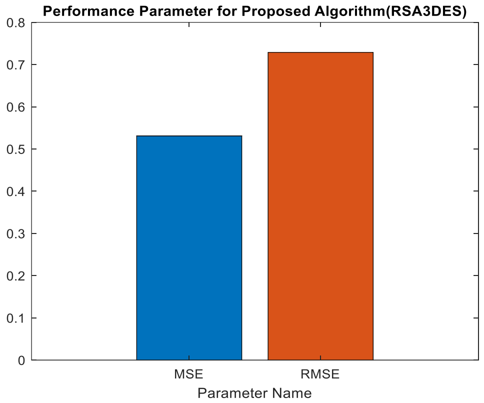


Figure 4: MSE and RMSE parameter's for RSA3DES

Mean squared error (MSE): The average squared disparity among the predicted values and the real ones is what is measured by the mean squared deviation (MSD) of an estimator (of a process for estimating an unobserved variable). As the expected value of the squared error loss, MSE is a risk function.

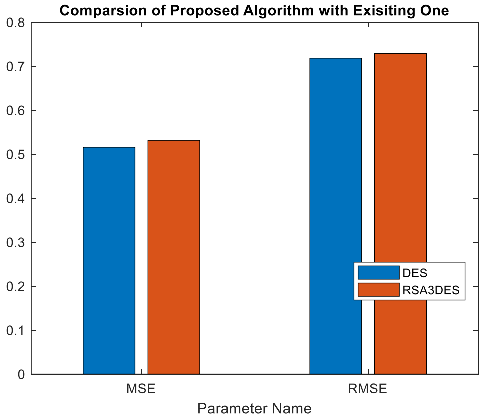


Figure 5: MSE and RMSE parameter's for DES

It is clearly shown from the 5 that the MSE and RMSE give the 0.52 and 0.71 values for the proposed approach and 0.5 and 0.71 for the existing one .

Root Mean Square Error (RMSE) is the residuals' standard deviation (forecasting errors). The distance between the data points and the regression line is measured by residuals, and the spread of these remainders is measured by RMSE. Put otherwise, it indicates the degree to which the data is centered around the line of best fit. In climatology, forecasting, and regression analysis, root mean square error is frequently used to validate experimental results.

Number of pixel change rate(NCPR): The difference among the proportions of positively and negatively charged residues is known as the NCPR parameter, and for AB_hRXG, it is equivalent to 0.014.

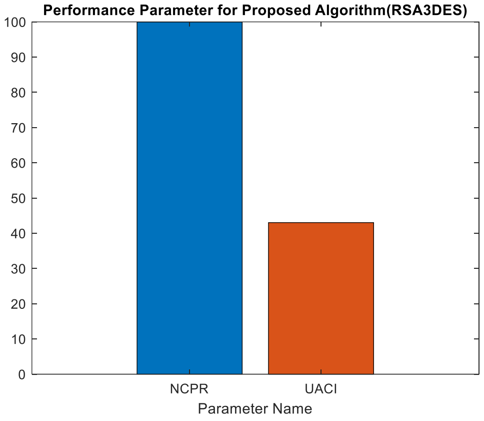


Figure 6:NCPR and UACI for RSA3DES

Unified Average Changing Intensity (UACI) : The UACI measure is employed to assess the resilience of picture encryption techniques against differential attacks. When two encrypted photos differ by just one pixel, it calculates the average change in pixel intensity between them.

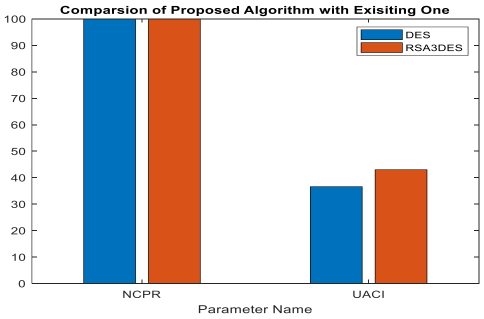


Figure 7:NCPR and UACI for DES

It is clearly shown from the figure 7 that the NCPR and UACI give the 100 and 45 values for the proposed approach and 100 and 38 for the existing one.

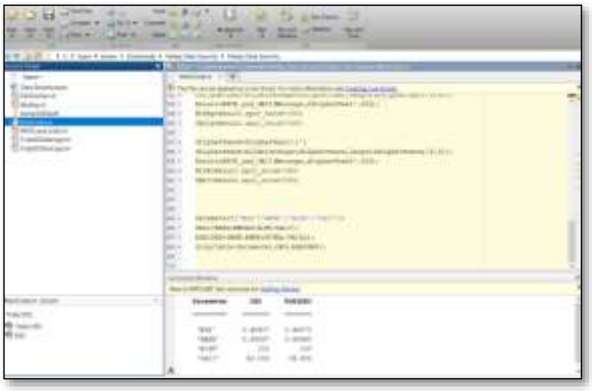


Figure 8: Data Security

Table 1 : Comparative analysis between the techniques

Parameter	DES	RSA3DES
MSE	0.48437	0.46875
RMSE	0.69597	0.68465
NCPR	100	100
UACI	42.082	34.498

It is evident from the numerical findings that the parameters MSE, RMSE, NCPR, and UACI provide the best results for the job that is being presented.

VI. CONCLUSION

The primary goal is to safely store and access data that isn't owned by the data owner on the cloud. Software structures often have multiple clients, a few endpoints, and one or more give-up servers. These exchanges take place over unstable networks between the client and the server. Communication takes place over open, public networks like the internet or private networks that could be compromised by adversaries from the outside or malicious insiders.

Cryptography may be employed to secure communications over untrusted networks. An adversary may try to assault a community in one of two primary ways. In a cloud computing environment, the existing data security techniques not only take longer to do operations, but they also give data less protection. It is evident from the numerical results that the

MSE, RMSE, NCPR, and UACI variables produce the best results for the given assignment.

REFERENCES

[1]M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.

[2]. P. S. Wooley, “Identifying Cloud Computing Security Risks,” Contin. Educ., vol. 1277, no. February, 2011

[3] V. J. Winkler, “Securing the Cloud,” Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.

[4] VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, “Single Cloud Security Enhancement using key Sharing Algorithm, ”Recent and Innovation Trends in Computing and 2016Communication, 2016.

[5]Emmanuel, A.; Aderemi, O.; Marion, A.; Emmanuel, A. A Note on Time and Space Complexity of RSA and ElGamal Cryptographic Algorithms. Int. J. Adv. Comput. Sci. Appl. 2021, 12, 143–147.

[6]Singhal, S.; Singhal, N. Comparitive Analysis of AES and RSA Algorithms. Int. J. Sci. Eng. Res. 2016, 7, 149–151.

[7] Alabi, O.; Thompson, A.; Alese, B.K.; Gabriel, A.J. Cloud Application Security using Hybrid Encryption. In *Communications on Applied Electronics (CAE)*; Foundation of Computer Science FCS: New York, NY, USA, 2020.

[8] Priya, C.; Kannan, M.; Vaishnavi, S. A comparative analysis of DES, AES and RSA crypt algorithms for network security in cloud computing. *J. Emerg. Technol. Innov. Res.* 2019, *6*, 574–582

[9] R, S. K., R, S., “Design of High Speed AES System for Efficient Data Encryption and Decryption System using FPGA”, International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT),2018.

[10] Sherif El-etriby, Hatem S. Abdul-kader, and Eman M. Mohamed, “Modern Encryption Techniques for Cloud Computing”, ICCIT, pp. 800-805, 2012.

[11] Dr. Nandita Sengupta, “Designing of Hybrid RSA Encryption Algorithm for Cloud Security”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, pp. 4146- 4152, May-2015.

[12] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A., “Cloud Security using Hybrid Cryptography Algorithms”, 2nd International Conference on Intelligent Engineering and Management (ICIEM),2021.

[13] Murali, G., & Prasad, R. S., “Comparison of cryptographic algorithms in cloud and local environment using quantum cryptography”,International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS),2017.

[14] Timothy, D. P., & Santra, A. K., “A hybrid cryptography algorithm for cloud computing security”, International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS),2017.

[15] Lee, B.-H., Dewi, E. K., & Wajdi, M. F., “Data security in cloud computing using AES under HEROKU cloud”, 27th Wireless and Optical Communication Conference (WOCC),2018.

[16] Amalarethinam, I. G., & Leena, H. M., “Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud”, World Congress on Computing and Communication Technologies (WCCCT),2017.