International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Secure Algorithm Using Encoding, Mathematical Key Generation and Redundancy in Cloud Computing

Rimpi Rani [1], Dr. Prof. R.K. Bathla[2]
[1] Assistant Professor Punjabi University TPD Malwa College, Rampura Phul,
Dist. Bhatinda Pb 151103 India
[2]Professor, Dash Bhagat University, Mandi Gobindgarh, Punjab India
Corresponding Author: rimpi.rani@pbi.ac.in

Abstract: This research paper explores the design and implementation of a customized encryption algorithm tailored to meet the unique security challenges of cloud computing environments. We discuss the algorithm's structure, customization options, and its potential benefits in enhancing data security within cloud-based applications. We introduce a tailored encryption algorithm that incorporates encoding, mathematical key generation and redundancy bits techniques to optimize data security, integrity, and efficiency within the cloud. A secure enhanced algorithm is developed. Customized encoding methods are employed to enhance data representation and facilitate efficient encryption and decryption. This includes the conversion of data into binary format for subsequent encryption. Redundancy bits are introduced into the encryption process to provide error detection and correction capabilities. The integration of these bits ensures data integrity, particularly during data transmission and storage. Random key is generated using Mathematical function. Experimental results demonstrate the algorithm's performance in terms of encryption and decryption times, file size comparisons, and data integrity measurements. Proposed Algorithm shows encryption time does not increases if the size of file bit increases. It increases only when size increases too much. It shows that encryption time is zero when size is small. With the increase of size decryption time also increases. When proposed algorithm is compared with traditional algorithm it takes less time. than RSA. However, encryption time and decryption time also depends on performance of system. Results may be differed. A novel algorithm is developed to improve the security of cloud computing. It has adopted three levels: the first level uses the Encoding Techniques. In second level: Redundancy bits are introduced Random key is generated using Mathematical function logical-mathematical function

Keywords: Cloud, Secure, Algorithm, Encryption, Decryption.

1. INTRODUCTION

Cloud computing is a new computing emerging technology that provides various services on demand at a low cost. The main goal of cloud computing is to provide easy-to-use, fast computing and data storage services but some risks and threats arise in the cloud computing environment. For enhancing the security of could computing, many techniques such as cryptography are used. Cryptography is in the transfer of data or messages secretly. It is also a way of converting the sender's letter into a secret term called the cypher text where only the intended recipient can learn the hidden message. Cryptology is a mathematical technique for security of data. Cryptography offers numerous more robust methods, and it is possible to use techniques to provide these security services. Encryption protocols, digital signatures, and hash functions various popular encryption algorithms are used to encrypt and decrypt confidential information that is represented by cryptography (Symmetric Algorithms, Asymmetric Algorithms, and Hybrid Algorithms).Moreover, to enhanced security issues in the cloud, this paper introduces a novel algorithm is developed to improve the security of cloud computing. It has adopted three levels: the first level uses the Encoding Techniques. In second level: Redundancy bits are introduced Random key is generated using Mathematical function logical-mathematical function Therefore, the major contributions of this paper can be summarized as follows: Section (1) presents an introduction. Section (2) presents a related work regarding the research. The novel proposed Algorithm has been implemented in Section (3). Section (4) shows the results and discussion are displayed. Section (5) describes the conclusions.

Objectives: To present a novel approach to address the security challenges posed by cloud computing through the customization of encryption algorithms.

2. RELATED WORK

Cloud computing is now active field of study. Cloud computing offers services like virtual data storage, collaboration, servers, networks, applications and tools with minimal resource commitment. The main concern of cloud computing is the security of data because vast volume of data is stored in the cloud storage. Data can be hacked or

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

destroyed by unauthorized users.[1] Cloud computing faces several security matters like service disruption, DoS attack, compromised authentication, and outside malicious insiders, security threats, system vulnerabilities, multi-tenancy issues, data integrity and data privacy [2]. Cloud security promises the protection of data or data failure. There are many malevolent users in the cloud, data protection may be at risk. Cloud Service also has to preserve data security to prevent unauthorized access of data in cloud storage. Incidents of data cracks or lack of data are common in these days [3] This author analyzed the data protection and privacy issues in cloud computing by intending on data isolation and secure privacy. Data security problems are of supreme significance to the extent and data of IaaS, PaaS and SaaS, which are core challenges in cloud computing. Data integrity is a serious enabler for cloud users. In addition to storing data, cloud technology also offers data management facilities. In data integrity, Many scholars are doing a lot of work on cloud data integrity and privacy issues [4]. Encryption is the main technology that pleases the criteria of security [5]. Various algorithms that are based on symmetric/asymmetric core technologies and genetic techniques such as RSA, DES, etc. are adopted, developed and applied [6]. Cryptographic algorithms can be compared based on their design, versatility, scalability, limitations and security, execution time, and memory requirements [7].

Research Gap: While customization trends are emerging, there remains a gap in comprehensive research that explores the design, implementation, and evaluation of customized encryption algorithms in the context of cloud computing. This paper seeks to address this gap by presenting a novel customized encryption algorithm and assessing its performance and security implications.

3. METHODOLOGY:

We introduce a tailored encryption algorithm that incorporates encoding, mathematical key generation and redundancy bits techniques to optimize data security, integrity, and efficiency within the cloud. A secure enhanced algorithm is developed. Customized encoding methods are employed to enhance data representation and facilitate efficient encryption and decryption. This includes the conversion of data into binary format for subsequent encryption. Redundancy bits are introduced into the encryption process to provide error detection and correction capabilities. The integration of these bits ensures data integrity, particularly during data transmission and storage. Random key is generated using Mathematical function.

This section outlines the methodology employed in the design, implementation, and evaluation of the customized encryption algorithm for cloud computing security. To address the unique security requirements and challenges of cloud computing environments, a secure enhanced algorithm is developed.

Encoding Techniques: Customized encoding methods are employed to enhance data representation and facilitate efficient encryption and decryption. This includes the conversion of data into binary format for subsequent encryption.

Redundancy Bit Integration: Redundancy bits are introduced into the encryption process to provide error detection and correction capabilities. The integration of these bits ensures data integrity, particularly during data transmission and storage.

Mathematical Key Generation: Random key is generated using Mathematical function

Algorithm Design and Implementation

The secure enhanced algorithm was designed and implemented. The algorithm consists of the following steps:

```
# Encryption Function
Function encrypt(data):
   # Data Encoding
   encoded_data = encode(data)
   # Redundancy Bit Integration
   data_with_redundancy = add_redundancy(encoded_data)
    return encrypted_data
# Decryption Function
function decrypt(encrypted_data):
   # Decryption
   decrypted_data = custom_decrypt(encrypted_data)
     # Redundancy Bit Removal
   data_without_redundancy =
remove_redundancy(decompressed_data)
   # Data Decoding
   original_data = decode(data_without_redundancy)
   return original_data
```

A controlled experimental setup is established to evaluate the customized encryption algorithm:

Data Sets: Diverse data sets, including text, images, and binary files, are used to assess algorithm performance across various data types.

Scenario-based Testing: Real-world cloud computing scenarios, such as data transmission, storage, and processing, are simulated to evaluate algorithm adaptability.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Testing Environment: The experiments are conducted in a controlled cloud computing environment using python language and anaconda prompt is used with appropriate security measures to ensure the integrity of the testing process. Various screen shots are taken and shown in figures. Figure 1 shows the output of code.

Figure 1 Output of Code

4. RESULTS AND DISCUSSION

Experimental results demonstrate the algorithm's performance in terms of encryption and decryption times, file size comparisons, and data integrity measurements. Proposed Algorithm shows encryption time does not increases if the size of file bit increases. It increases only when size increases too much. It shows that encryption time is zero when size is small. With the increase of size decryption time also increases. When proposed algorithm is compared with traditional algorithm it takes less time. than RSA. However, encryption time and decryption time also depends on performance of system. Results may be differed.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

The performance and effectiveness of the algorithm are assessed and shown in table 1

Encryption and Decryption Times: The time required for encryption and decryption processes is measured to evaluate algorithm efficiency.

File Size Comparisons: File sizes before and after encryption are compared to assess the impact of customization on data size.

Algorithm	File Size	Encryption Time	Decryption Time
AES	177	0.005002	0.011007
AES	2067	0.00973	0.005006
AES	5331	0.01077	0.007006
RSA	177	0.000973	.005006
RSA	2067	0.001073	.006006
RSA	5331	0.001173	.007006
Proposed Enhanced Secure Algorithm (PESA)	177	0.001003	0.00000
Proposed Enhanced Secure Algorithm	2067	0.003003 0.004000	0.002037
Proposed Enhanced Secure Algorithm	5331	1.178696	.007006

Table 1(Algorithm, file size, Encryption 1

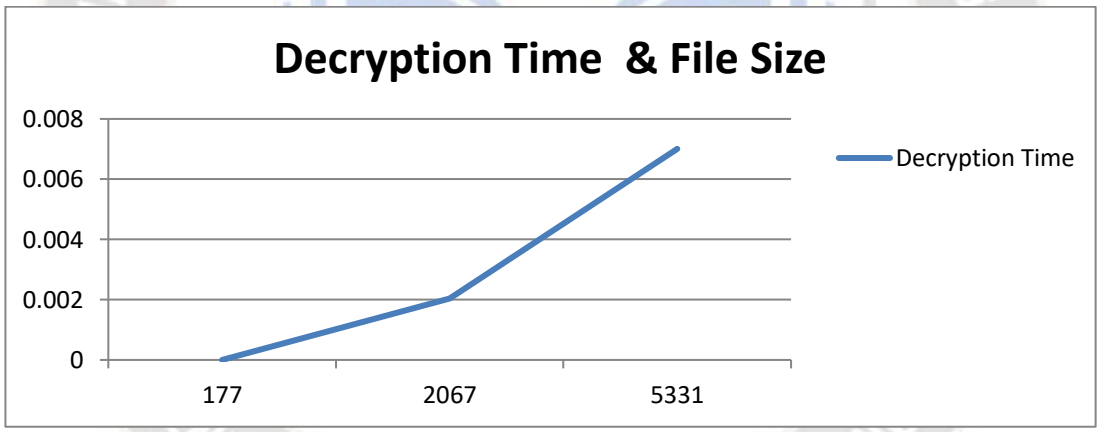

Chart 1 Decryption Time & File Size

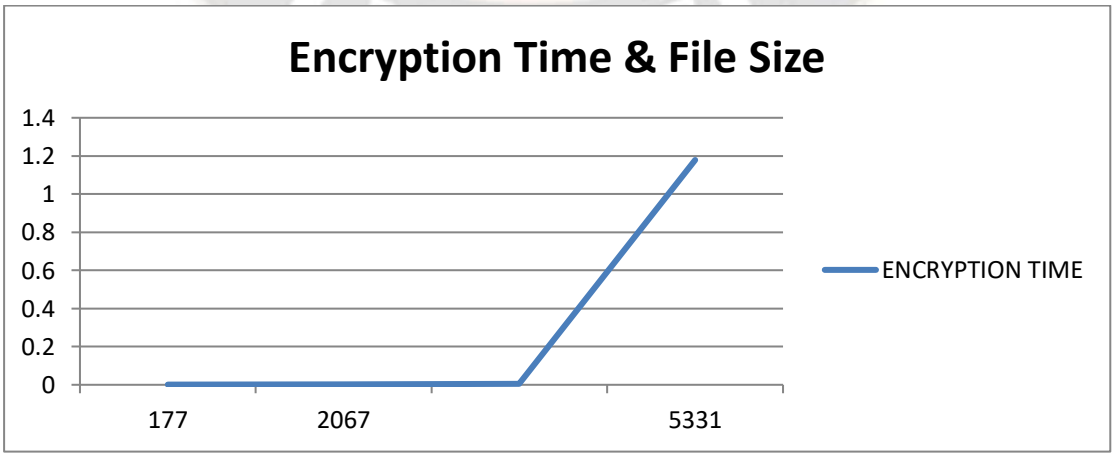

Chart 2 Encryption Time & File Size

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

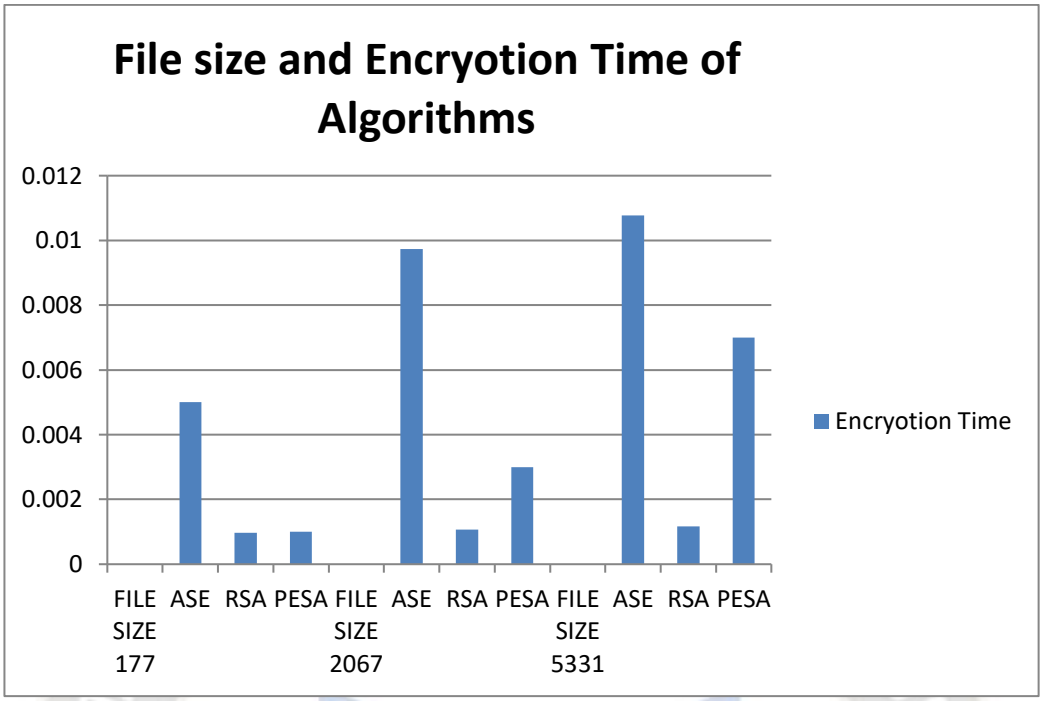

Chart 3 File size and Encryptions Time of Algorithms

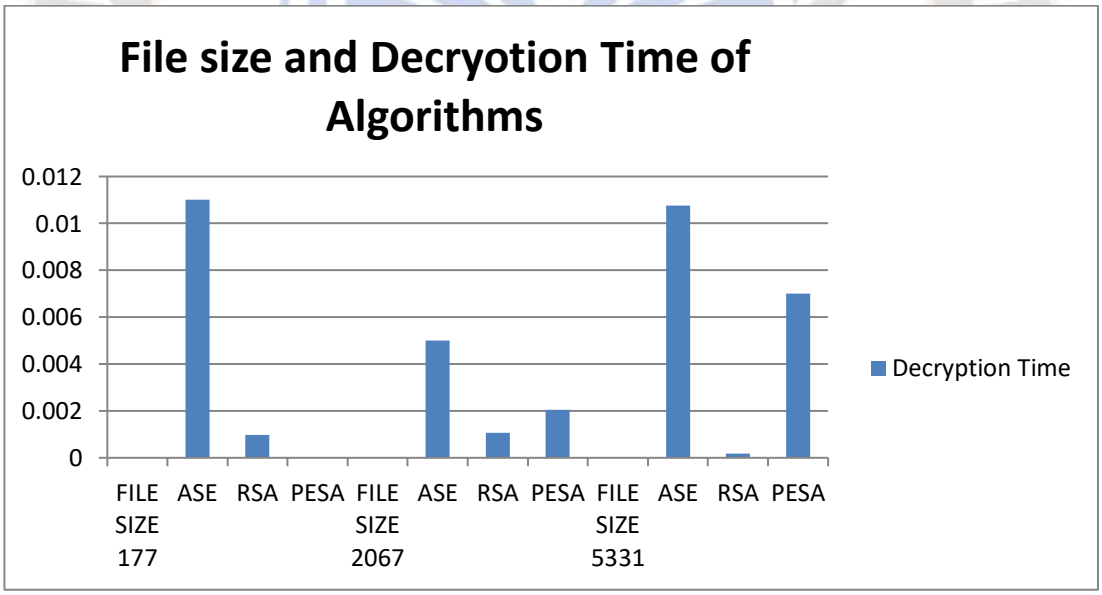

Chart 4 File size and Decryption Time of Algorithms

Proposed Algorithm shows encryption time does not increases if the size of file bit increases. It increases only when size increases too much (shown in chart 1). It shows that encryption time is zero when size is small. With the increase of size decryption time also increases (shown in chart 2). When proposed algorithm is compared with traditional algorithm it takes less time. than RSA (shown in chart 3 & 4). However, encryption time and decryption time also depends on performance of system. Results may differ it is shown in table too.

Cloud Deployment of Algorithm

For deploying algorithm Cloud Service Provider Google Cloud Platform was chosen and account was set up. Data files can be uploaded and downloaded.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

Testing is performed in the cloud environment to ensure algorithm works as expected. We successfully deploy our algorithm in a cloud computing environment while considering security, scalability, and cost-effectiveness. Various screen shots of Cloud Deployment are taken and shown in figures. Fig 3 shows the uploaded files on Google Coud. Fig 4 shows output of downloaded encrypted file. After encryption file is uploaded . We can download encrypted file and then decrypt it.

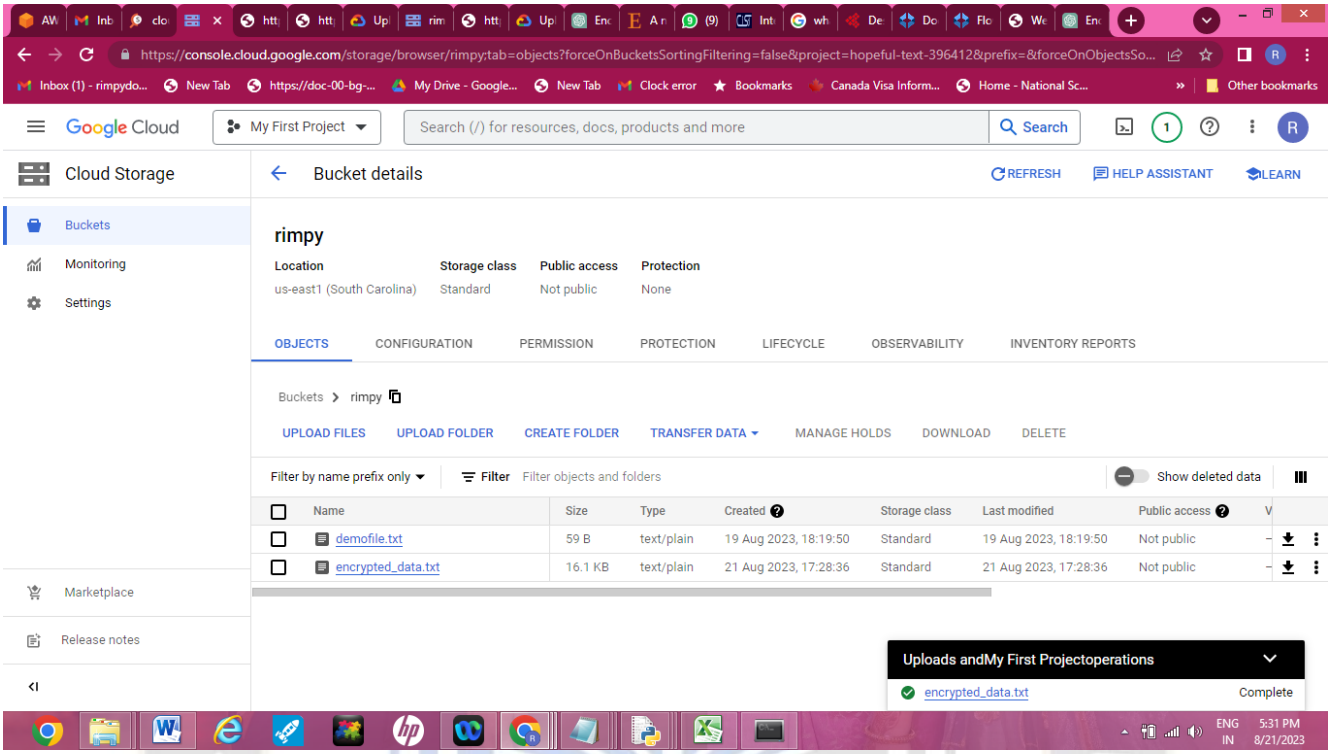

Figure 2 Screen shot of cloud deployment

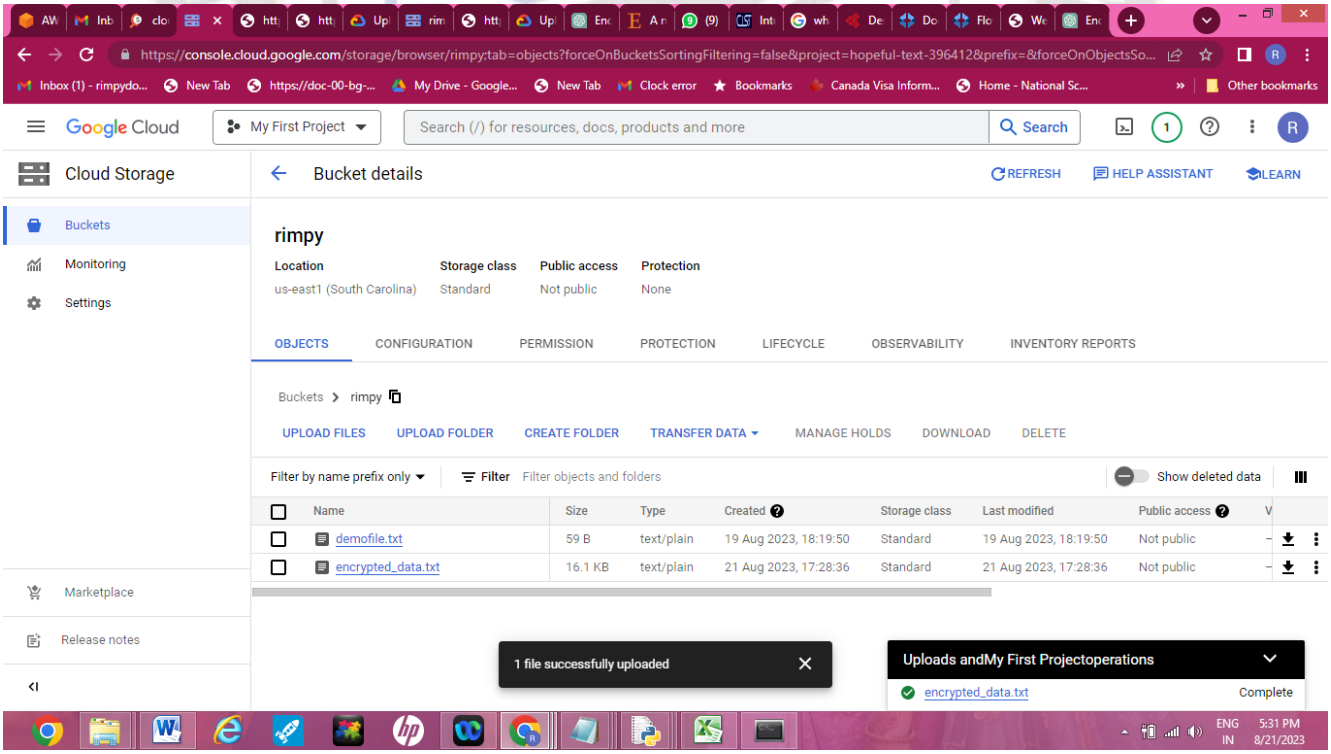

Figure 3 Screen Shot of Cloud Deployment

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

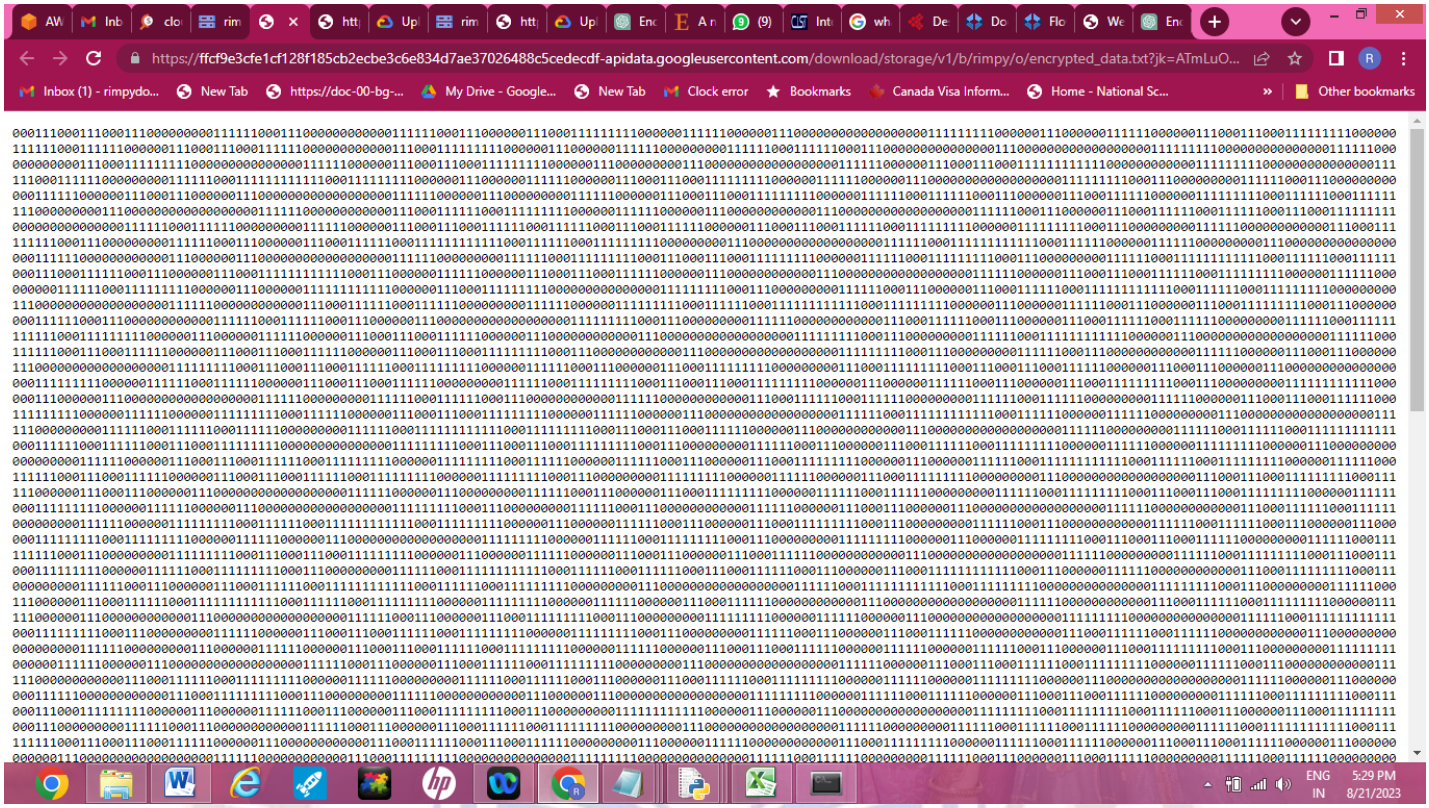

Figure 4 Encrypted File Downloaded From Cloud 1

Proper key management practices are implemented to ensure data security and confidentiality throughout the encryption process. This includes secure key generation, storage, and distribution. Additionally, security considerations are addressed, including potential vulnerabilities and threat mitigation strategies.

Data Integrity Measurements: The effectiveness of redundancy bits in detecting and correcting errors is evaluated by introducing controlled data corruption scenarios

The superiority of proposed algorithm for cloud computing can be evaluated based on several key factors and advantages it offers compared to existing encryption approaches. Here are some ways in which your algorithm may be considered better:

Enhanced Security: It may provide additional security layers, such as redundancy bits and specialized encoding, making it more robust against attacks and data breaches.

Error Detection and Correction: The inclusion of redundancy bits allows your algorithm to detect and correct errors in the encrypted data, ensuring data integrity during transmission and storage.

Efficiency: Encoding techniques can optimize the size of encrypted data, reducing storage and bandwidth requirements, which can be especially beneficial in cloud environments with limited resources.

Adaptability: This algorithm's framework enables it to adapt to various cloud computing scenarios, making it versatile for different applications and use cases.

Scalability: The algorithm's design may support efficient scalability, allowing it to handle increasing workloads as cloud resources are scaled up or down.

Resource Efficiency: Algorithms can be tailored to the specific resources and requirements of the cloud environment, optimizing resource utilization and minimizing costs.

Data Privacy Compliance: Custom encryption and security measures can be designed to meet specific data privacy regulations, helping organizations comply with legal requirements.

Customization for Specific Use Cases: This algorithm can be fine-tuned for particular use cases within cloud computing, ensuring that it meets the unique needs of different applications and industries.

Performance Optimization: By designing your algorithm to align with the cloud architecture and infrastructure, we can achieve better performance and reduced latency in data encryption and decryption processes.

Cost Savings: Resource-efficient algorithms can lead to cost savings in terms of cloud resource usage, data storage, and data transfer fees.

Flexibility and Control: Your algorithm's customization framework gives you greater control over security measures, allowing you to adapt to evolving threats and requirements.

Ease of Integration: A well-designed algorithm can be integrated seamlessly into existing cloud infrastructure, minimizing disruption to operations.

Versatility: This algorithm's adaptability can make it suitable for a wide range of cloud computing scenarios, from data storage and processing to real-time applications.

5. CONCLUSION

A novel algorithm is developed to improve the security of cloud computing. It has adopted three levels: the first level uses the Encoding Techniques. In second level: Redundancy bits are introduced Random key is generated using Mathematical function logical-mathematical function. The proposed secure encryption algorithm tailored for cloud computing offers several significant advantages that make it a valuable addition to the field of data security and cloud services. This algorithm has been designed with a focus on enhancing security, efficiency, and adaptability, making it better suited for the unique challenges and opportunities presented by cloud computing environments.

REFERENCES

1. M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: opportunities and challenges, Inf. Sci. (2015), https://doi.org/10.1016/j.ins.2015.01.025.
2. N. Kshetri, Privacy and security issues in cloud computing: the role of institutions and institutional evolution, Telecommands. Pol. (2013), https://doi.org/10.1016/ j.telpol.2012.04.011.
3. D. Chen, H. Zhao, Data Security and Privacy Protection Issues in Cloud Computing, 2012, https://doi.org/10.1109/ICCSEE.2012.193.
4. S. Pearson, A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2010, https://doi.org/10.1109/CloudCom.2010.66.
5. A. Bhardwaj, G.V.B. Subrahmanyam, V. Avasthi, H. Sastry, Security Algorithms for Cloud Computing, 2016, https://doi.org/10.1016/j.procs.2016.05.215. F. Thabit et al. International Journal of Intelligent Networks 2 (2021) 18–33 32
6. P. Dixit, A.K. Gupta, M.C. Trivedi, V.K. Yadav, Traditional and hybrid encryption techniques: a survey, in: Lecture Notes on Data Engineering and Communications Technologies, 2018.
7. S. Chowdhury, S.R. Ghosh, A. Paul, Design and implementation of a novel cryptographic technique for network security using genetic algorithms (gas), Int. J.