A Secure and Efficient Cloud Storage System Using Advanced Encryption Standard Algorithm for Data Protection

Gurujukota Ramesh Babu, Phaneendra Varma Chintalapati(✉), Pokkuluri Kiran Sree, Kode Satish Kumar, A. V. S. Asha, and Boddu Maneesha

Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, Bhimavaram, India
{grameshcse,chpvarmacse}@svecw.edu.in

Abstract. The Cloud Computing (CC) is a model which treats the resources as an integrated entity on the internet, cloud. Cloud computing is an unique environment or network in which process, access and maintenance are done by anywhere from the world. The CC is a customized internet-based web server. Data security is receiving more and more attention with the expanding usage of cloud storage systems and due to its challenging circumstances. Any cloud data storage model's fundamental objective is to provide simple data access without compromising the security of the data. The main concerns of any cloud storage system are ensuring safety and security. Big data security and privacy have emerged as a problem that prevents the usage of cloud services by the organization. Earlier privacy-preserving methods had a number of drawbacks includes completely dependence on third parties, a lack of performance efficiency, accurate data analysis, and data privacy. This analysis presents a secure and efficient cloud storage system that uses the advanced encryption standard algorithm for data protection. The user files are encrypted with the AES (Advanced Encryption Standard) standard. The efficiency of the method that is being provided is evaluated in terms of execution, decryption, and encryption times.

Keywords: Cloud Computing · Big data · Data Privacy and Security · Advanced Encryption Standard (AES)

1 Introduction

In recent years, the term "big data" has been used frequently at a higher rate. The utilization of big data is extensive in present social production and is important to the advancement of industrial companies and reforms. As all know that, big data makes lives more convenient while also brings certain security and privacy dangers [1]. Higher standards for information processing have been prompted by the growth of data and its use which leads to security and privacy concerns that have attracted a lot of attention. Every Internet activity is tracked in the big data, since if it is revealed, it will harm people in particular manners [2].

P. Pareek et al. (Eds.): IC4S 2024, LNICST 598, pp. 72–83, 2025.
https://doi.org/10.1007/978-3-031-77078-4_6

Due to its capacity for storage (beyond the size of a typical database), retrieval, analysis, and the ability to create relevant results, the term "big data" was recently coined and gained popularity. The amount is massive and poorly organized, making it difficult to understand since it is always expanding in real time. The changes in technology influence the classification changes of such data [3].

The cloud computing has shown a whole new way for file storage to the world. The CC can be characterized by self-services, on demand, network accessibility, resource sharing, and other services define cloud computing. Cloud computing aims to reduce costs, enable customers to utilize all of the cloud's capabilities, and assist them in concentrating on their primary businesses. By connecting the computing and storage resources managed by several operating systems, customers can utilize services like high-performance computers and extensive data storage due to cloud computing. Due of this feature, cloud computing is a great candidates for adoption by companies, organizations, and individual users. The concept of cloud computing has been a focus of numerous research, many of which have concentrated on particular issues and challenges [4].

A virtual storage system known as cloud storage allows information to be stored and accessed from virtual servers rather than actual servers, the conserving storage space. Users have the option of maintaining and handling their data in data centers owned and operated by other parties due to cloud storage and processing. Cloud computing is used by organizations in many different models of services [5]. Data is remotely maintained, managed, and backed up in a cloud environment and then made available to end users through the internet in a cloud storage service. It enables the customer to acquire the files online, allowing the client to access these files from any location through the internet. To store and remotely access their data from any location at any time without generating additional charges, businesses and consumers use cloud storages in cloud data centers [6].

One of the most preferable computation models for big data operations is Cloud deployment models. This trend is motivated due to their flexibility, cost-effectiveness and scalability. However, in such models, the data were no longer maintained physically under the direct control of users which can leads to new security concerns [7]. The confidential information that privileged users, including corporations and governmental organizations, in the public cloud is very exposed to hackers and cloud service providers [8]. Security and privacy of cloud data are major issues. Making sure of the data integrity, privacy, and safety is essential for a service in the cloud. Depending on the nature, scale, and type of the data, a number of service providers utilize an extensive number of regulations and processes for this reason [9].

Less privacy, incorrect data analysis, and complete depend on outside parties are just a few disadvantages of previous privacy-preserving methods. Security breaches and unauthorized access events have happened with several public and private cloud services. Big data generates significant and important concerns about data privacy [10]. The improper use of private data, especially when it is combined with data from other sources, it is widely recognized by the general public. To use big data effectively, people must recognize that handling privacy is a socio-technical issue [1]. Secure storage of sensitive data is essential to modern communication, especially when using the cloud. Individuals with use cloud computing services are utilizing it more often every day, and

cloud computing environments have been used to store a lot of information. Hence to overcome these issues, encryption is come into picture [11].

Encryption is the process of transforming plain text into a format that cannot be read. Biometrics are used in computer science and engineering, particularly as an access control and personality test [23]. The data is kept in various storage facilities that the specific data distributors will keep track on information. The data is retrieved from the cloud storage in a reversible manner if the authorized user is accessing the information. Encryption is used to satisfy the needs of information exchange, data secrecy, and security [12]. There have been many new cryptographic algorithms created recently, but for a secure cloud environment, select the widely recognized as highly secure data encryption standards (DES) or rivest, shamir, adleman (RSA). However, the repetition of cloud data values in cipher text or another language known as patterns are one of the alternatives. Following the generalization of the coding process by deep analysis, any intelligent intruder may quickly identify these patterns. Hence, an efficient encryption algorithm is essential for secured cloud storage and data protection [13].

In this work, an advanced encryption standard method for data security is used to create a safe and effective cloud storage system. The text that remains is as follows: Sect. 2 provides a description of the literature review. A secure and efficient Cloud Storage system using advanced encryption standard algorithm for data protection is described in this Sect. 3. The analysis of the results is evaluated in Sect. 4. Section 5 provides the conclusion to the analysis.

2 Literature Survey

Shen J, Zhou T., He D., Zhang Y., Sun X. and Xiang Y. et al. [14] explains Cloud Computing's Block Design-Based Key Agreement for Group Data Sharing. A novel block-based key agreement protocol that is capable of supporting numerous participants is demonstrated. This model easily extended the participants in the cloud platform in accordance with block design structure. The common conference key for n participants is generated using a defined group data sharing approach, based on which general formals are described. The computational complexity of the proposed protocol increases with the number of participants when utilizing the block design, while communication difficulty is significantly reduced.

Li Xiang, Ning Zhang, Xiao Lan, Qixu Wang, Xingshu Chen, and Dajiang Chen et al. [15] explains the combination of reputation management and security help increase the security of trusted cloud services as well as cloud-based IoT security. Utilizing a combination of reputation- and security-based reliable evaluation techniques, to maintain the IoT environment's cloud-based security, this framework enables evaluating the dependability of cloud services. Utilizing certain security metrics, a cloud service's security is evaluated to clouds using the security-based trust evaluation methodology. This trust assessment methodology may more successfully and more effectively measure a cloud service's trustworthiness than earlier trust evaluation methods, according to tests utilizing simulated security metrics data and data from actual online services.

Parinya Suwansrikham, Kun She et al. [16] proposes a secure asymmetric storage method for large amounts of data across many cloud providers. This study outlines

ways to reduce risk, maintain data privacy, and gain controlling. Multiple cloud storage providers get the enormous data file once it has been divided into portions. Despite the fact an insider attacks occurs, just a portion of the material is obtained. Attacker is unable to fully rebuild the file. Metadata is produced after the file has been divided. The study in this area uses the notion of asymmetric security. The person who asks access to the file receives the encrypted metadata. File accessing is one of dew computing's roles as an intermediary server between cloud users and cloud services, monitoring, and metadata transmission.

Talal Halabi and Martine Bellaiche et al. [17], a game-theoretic method is demonstrated through the security- based establishment of cloud federations. A cloud federation development approach that takes into consider the security posture of cloud service providers (CSPs) is presented by the authors in this study. With regard to a specified Security-SLA (Service Level Agreement) baseline and taking into consideration the protection satisfaction of CSPs peoples, the CSPs and newly formed federations security levels were evaluated. This solution initially applies the goal-question-metric (GQM) approach to offer a set of parameters that quantitatively describe the security-SLA (security level agreement) in the Cloud. They offer a federation construction method that allows CSPs to join federations while minimizing security losses and avoid creating federations that are generally unsafe. According to the experimental results, through reducing the frequency and seriousness of Security-SLA violations, this strategy helps maintain better security standards in newly formed federations.

El-Booz S.A., Attiya G. and El-Fishawy N. [18] explains an automated preventing protocol-based secure cloud storage system with a time-based one-time password. The presentation of a different secure cloud storage system ensures organizational data privacy from the cloud provider, the external auditor, and specific users who may access the data saved on the cloud using their old files. The two authentication techniques used by the proposed system to increase the level of authentication security are automated blocker protocol (ABP) full protection against audits by unauthorized third parties and time-based one-time password (TOTP) for cloud user verification. The experiment results demonstrate the efficiency of the suggested system in confirming the accuracy of shared data.

Gai K., Qiu M. and Zhao H. et al. [19] explains a mass distributed storage method for massive data clouds that is both effective and security-aware. The suggested paradigm, often described as the security-aware efficient distributed storage (SAEDS) model, is based primarily on the secure efficient data distributions (SED2) algorithm and the efficient data conflation (EDCon) technique. Performances in terms of efficiency and security have both been evaluated experimentally.

3 Secure and Efficient Cloud Storage System

A secure and efficient cloud storage system using advanced encryption standard algorithm for data protection is presented in this section. In Fig. 1, the provided system's block diagram is displayed. Data selection is the first stage in this process. The file is uploaded by the data owner, who then encrypts it and stores it on the server. The user must fill out the registration form to establish a new account if they don't already have

account. The username and password are given if the user already exists, and the file is uploaded. By implementing TDES (Triple Data Encryption Standard) encryption and cloud storage, the file is encrypted before being saved.

The real-time healthcare dataset is used in this analysis to conduct an experimental examination. The dataset has 3024 instances and 17 attributes, including the gender, patient's name, age, month, symptoms, location, disease, maximal heart rate reached, serum cholesterol, body mass index derived from a resting electrocardiogram, name of consultant, type of work, height, and weight, as well as past medical history. The necessary data are chosen and taken into consideration for the encryption procedure based on the characteristics of the patients. Prior to encrypting the data, the administrator generates a mask for the qualities relating to the personal information, such as name, age, gender, and month of the patient; past medical history; location; type of job; body weight; and consultant name. The data is portioned according to data sensitivity as low sensitive, medium sensitive and high sensitive data. After data partitioning, the following step involves input encryption using the Triple Data Encryption Standard (TDES) technique. A common and open encryption mechanism with 112 bits and a strength of 168 bits for encryption is called TDES. Symmetric key models are used by TDES for data transmission, reading, and writing. TDES offers greater protection and uses symmetric key creation, which makes it effective.

Although the TDES has big size key lengths that are longer than those of earlier encryption schemes, it is a useful technology for both encryption and decryption. Block cipher algorithms are used three times to each block in the TDES manner in which encryption. The TDES is an encryption standard that uses symmetric block ciphers and fixed length keys with three phases. The key size of TDES is increased to ensure additional security through encryption capabilities. TDES has proved its reliability and a longer key length which eliminates many of the attacks. The data is maintained as big data after encryption. TDES encryption is generally described as

$$E^1 = E^3 = E,\ E^2 = D \tag{1}$$

TDES uses three different encryption methods: E^1 for single encryption, E^2 for double encryption, and E^3 for triple encryption and D is counterpart of decryption. Cloud platforms store the encrypted health data. The read-write storage activities are efficiently supported by the cloud. Clustered or scale-out network attached storage, redundant and scalable direct connected storage pools, or it will mostly be utilized as object format storage make up big data infrastructure. Big data measures may be processed and retrieved more quickly due to a connection between the big data infrastructure and cloud computing server nodes. Utilizing Spark over the Hadoop distributed environment allows for the easy distribution of encryption keys to worker machines and the provision of cloud-based memories. Key servers and distributed storage servers make up the distributed storage system. Security measures have been taken to keep these important servers extremely secured.

Whenever user requests the respective file is forwarded and selected file is encrypted using AES. The data is kept in various storage facilities that the specific data distributors will keep a track on the information. Data is reversibly recovered from the cloud storage, whether the permitted user is using the data. In order to fulfill the needs of data

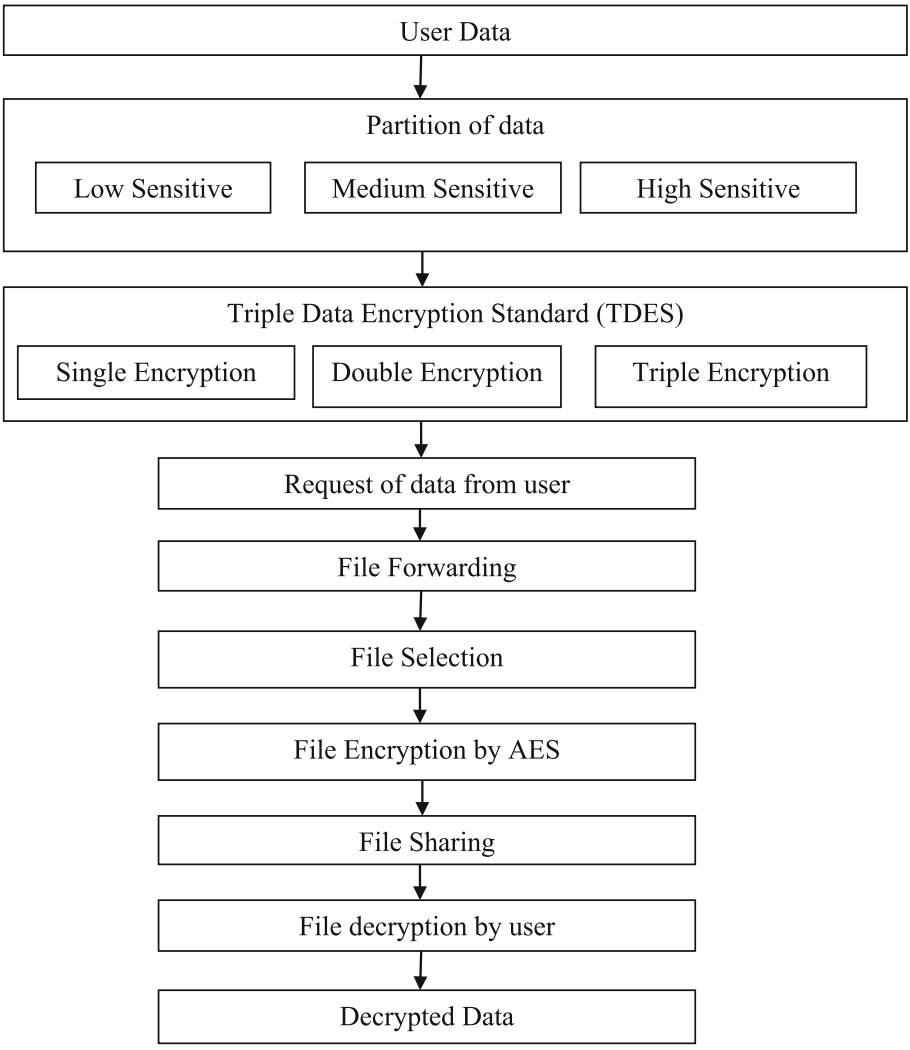

Fig. 1. Block Diagram of Secure and Efficient Cloud Storage System using AES

confidentiality, security, and information sharing, erasure coding and encryption can be applied.

Whenever upload a file to the cloud, the user establishes a login. Following account creation, the user browses for the file to upload, uploads the file to the cloud after that. Implementing the AES technique, the file is encrypted. The client chooses the file they want to download, and then the file is decrypted. When sharing files, AES encryption is used to protect information. The user can share the file with a recipient and store it on their system. The recipient downloads the file, logs into the account, and decrypts it. This limits security breaches while the file is transmitted.

The symmetric encryption method known as Advanced Encryption Standard (AES) generates keys with 128 bits (for this purpose). Since AES uses many encryption rounds, it provides security by making the encrypted data more difficult to extract and more difficult for threat actors to intercept or steal. This process is effective for both software and hardware. The AES protocol is used to encrypt the given material. This method has thus far been demonstrated to be safe and has essentially not been compromised. In this study, as a result of its smaller quantity, a 128-bit key is utilized (10 rounds), which makes processing simpler and faster. AES places the 16-byte (4-byte X 12-byte) grid in columns for each block. Add Round Key, Mix Columns, Sub-Bytes, and Shift Rows are the four steps that make up each round. The Mix-column round is absent from the previous round. Row shifting and substitution are handled by the sub-byte. In the model, Mixcolum performs the permutation. Sub Bytes: The substitution is carried out at this stage. Every byte is replaced with a different byte during this operation. S-box, also known as look-up tables, is used for changing sub-bytes. As before, a 16 byte (4×4) matrix is the result of this method. Row Shift: In this procedure, a specific number of times is shifted for each row. There is no shift in the first row. One shift is made to the second row's left. Three shifts are made to the fourth row's left. Mix-Column: This usually involves multiplying matrices. Each byte column location is altered as a result of multiplying each column by a particular matrix. Add Round Key: Adding round key is the last step. After all of these rounds are finished, the encrypted data is sent as output. The output from the previous step is XORed with the matching round key. The cloud storage will keep each data fragment in a distinct location. The public distributor keeps track of all the data and the locations where it is kept. A reversible response will be given by the cloud system when a real client requests the information. Therefore, this approach can protect the information submit from both internal and external threats and attacks.

The cloud environment data are obtained during the data decryption process using TDES approach. The data owner can access the Cloud of healthcare organizations using the TDES technique. Owners of the data can visit the Hadoop cluster resources manager to get their data. The resource manager will be able to distribute the enormous data tables across different data nodes or providers. Using the proper decryption key for each feature, the data in the TDES method is decrypted based on the security level. TDES reads each attribute's security level in a comparable way. When TDES is finished, data encrypted by users is decrypted by Hadoop and stored in the output directory. Hence, this system effectively encrypts the data and stores into the cloud. The data is decrypted whenever user requests. This approach has the benefit of promoting the exact integration of encoding, encrypting data and developing data, allowing for the creation of a storage system that is capable of fulfilling the demands of information interchange, data privacy, and data security.

4 Result Analysis

A secure and efficient Cloud Storage system using advanced encryption Standard algorithm for data protection is implemented in this section. Below is a description of the few security measures that can be taken to enhance the cloud computing environment:

This analysis makes use of a real-time healthcare dataset with 17 features. The user data is encrypted using TDES. Data is saved in the cloud after encryption. When a user requests data, it is obtained from the cloud and encrypted with AES before being shared with the user. TDES is used to decode the data. In order to create a storage system that properly supports information protection, it promotes the precise integration of encoding, encryption, and advancement in order to maintain data privacy and information exchange.

The following is a description of the security procedures that are utilized to enhance cloud storage:

Execution Time: For particular tasks, execution time is also referred to as CPU time, this is the amount of time the system needs to do the task.

$$Execution\,Time = 1 * CPI * T \tag{2}$$

I denote the total number of program instructions, T refers for the duration of a clock cycle, while CPI stands for the average number of Cycles Per Instructions CPU utilization. Table 1 indicates the performance comparison in terms of execution time and CPU utilization.

Table 1. Performance Comparison

Methodologies	Execution Time (ms)
Efficient mass Distributed Storage (EDS) for cloud systems with big data with security awareness	16000
Presented secure and efficient cloud storage system using advanced encryption standard algorithm for data protection	12000

Table 1 displays the performance of the suggested strategy against the existing methods in terms of execution time, CPU consumption, and network use. The time needed for the encryption, transport, and decryption of medical data is included in the execution time of the current approach. The CPU is used during end-to-end execution to improve performance and conform to security standards. Figure 2 shows the execution time comparison.

In Fig. 2, the x-axis represents different cloud storage system whereas y-axis represents execution time in ms (milli seconds). Table 2 presents a comparison of the encryption and decryption times for various methods.

As compared to enhancing cloud data security using a hybrid verification method that combines encryption and biometrics, presented approach using AES requires less encryption time as well as decryption time. Figure 3 shows security and privacy comparison.

Fig. 2. Execution Time Comparison

Table 2. Encryption and Decryption Time Comparison

Text files size (kb)	Improving cloud data security through hybrid verification technique based on biometrics and encryption system		Presented secure and efficient cloud storage system using advanced encryption standard	
	Encryption Time (ms)	Decryption time (ms)	Encryption Time (ms)	Decryption time (ms)
200	30	31	25	26
400	35	35	27	27
600	44	46	38	39
800	52	52	46	47
1024	58	59	49	50
2048	85	91	78	79

Compared to earlier EDS storage system, this model has provided better privacy and security to the data which is stored in big data and cloud platforms. The encryption time comparison graph is displayed in Fig. 4, with the file size in Kb (Kilo bytes) on the x-axis and the encryption time in ms on the y-axis.

Compared to cloud data security using hybrid verification technique based on biometrics and encryption system, the presented approach utilizing AES takes less time for encryption. The decryption time comparison graph is shown in Fig. 5, with the file size in Kb (Kilo Bytes) on the x-axis and the decryption time in ms (milliseconds) on the y-axis.

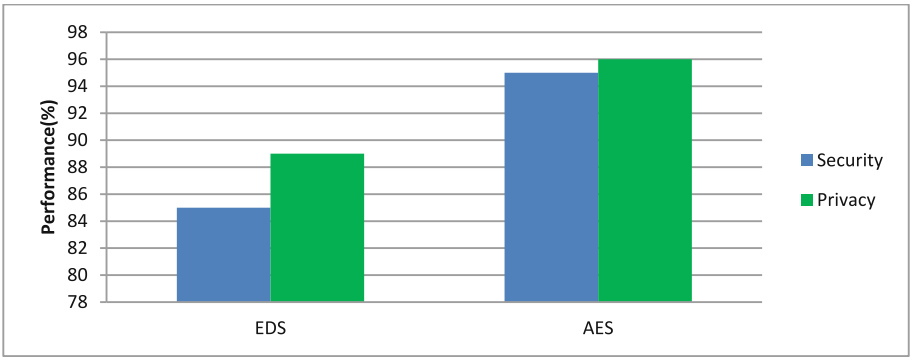

Fig. 3. Security and Privacy Comparison

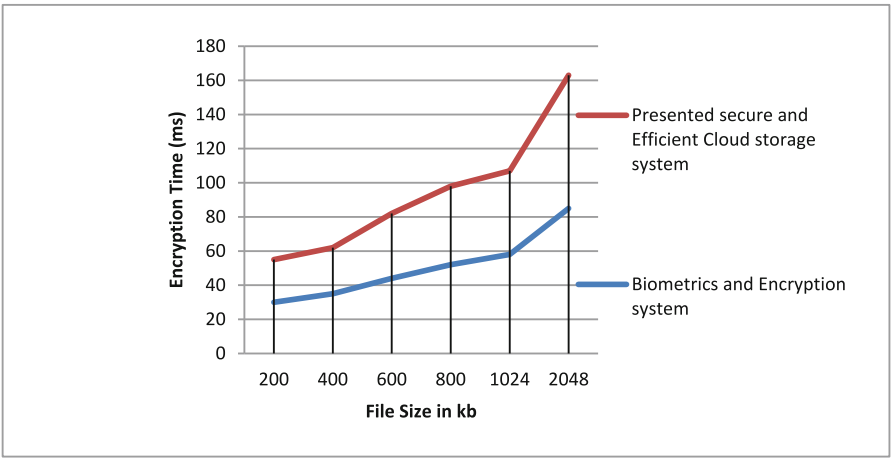

Fig. 4. Encryption time Comparative Graph

Compared to cloud data security utilizing a hybrid verification technique based on biometrics and encryption system, the presented approach utilizing AES requires less time to decrypt data. Therefore, presented secure and efficient cloud storage system using AES has effectively provided the data protection, confidentiality and security. In addition, it requires less time for encryption as well as decryption.

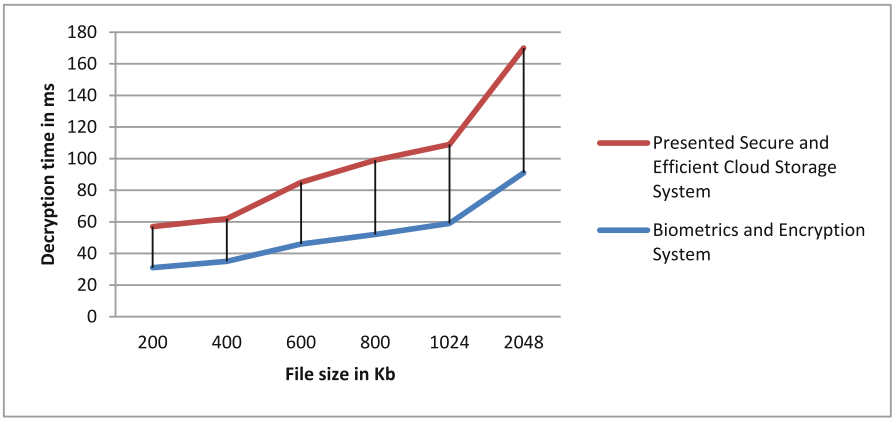

Fig. 5. Decryption Time Comparison

5 Conclusion

A secure and efficient cloud storage system using advanced encryption standard for data protection is presented in this analysis. In this analysis, real time health dataset is used. The user uploads the data through their accounts. The uploaded data is portioned according to the level of data sensitivity and is encrypted using TDES. Whenever user requests the data, then the appropriate data file is selected and is encrypted through Advanced Encryption Standard. The information is being accessed by an authorized user, it is recoverable from the cloud storage in a reversible way. This system has provided better data protection, data confidentiality than earlier approaches, since it encrypts the data two times using TDES and AES. The execution time, encryption time, security, privacy and decryption time of the system under consideration are all measured in terms of performance. Compared to earlier cloud storage systems, this system have requires less execution time less encryption and decryption Time. Hence presented system has effectively provided the data protection and confidentiality to user data.

References

1. Sasikumar, A., Ravi, L., Kotecha, K., Abraham, A., Devarajan, M., Vairavasundaram, S.: A secure big data storage framework based on blockchain consensus mechanism with flexible finality. IEEE Access **11**, 56712–56725 (2023)
2. Dang, D.T., Hoang, D., Nguyen, N.D.: Trust-based scheduling framework for big data processing with MapReduce. IEEE Trans. Serv. Comput. **15**(1), 279–293 (2022)
3. Rawat, B.D., Doku, R., Garuba, M.: Cybersecurity in big data era: from securing big data to data-driven security. IEEE Trans. Serv. Comput. **14**(6), 2055–2072 (2021)
4. An, S., Leung, A., Hong, B.T., Eom, T., Park, S.J.: Toward automated security analysis and enforcement for cloud computing using graphical models for security. IEEE Access **10**, 75117–75134 (2022)
5. Antony Joans Kumar, M., Christopher Columbus, C., Ben George, E., Ajith Bosco Raj, T.: A virtual cloud storage architecture for enhanced data security. Comput. Syst. Sci. Eng. **44**(2), 1735–1747 (2023)

6. Du, J.: Analysis of a joint data security architecture integrating artificial intelligence and cloud computing in the era of big data. In: 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 988–991 (2022)
7. Awaysheh, M.F., Aladwan, N.M., Alazab, M., Alawadi, S., Cabaleiro, J.C., Pena, F.T.: Security by design for big data frameworks over cloud computing. In: IEEE Transactions on Engineering Management, pp. 3676–3693 (2022)
8. Funde, S., Swain, G.: Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies. IEEE Access 105458–105484 (2022)
9. Amr Sauber, M., Passent M., El-Kafrawy, Amr Shawish, F., Mohamed Amin, A., Ismail Hagag, M.: A new secure model for data protection over cloud computing. Comput. Intell. Neurosci. 1–11 (2021)
10. Shen, J., Liu, D., Liu, Q., Sun, X., Zhang, Y.: Secure authentication in cloud big data with hierarchical attribute authorization structure. In: IEEE Trans. Big Data 668–677 (2021)
11. Morales-Sandoval, M., Cabello, H., Marin-Castro H., Compean, J.: Attribute-based encryption approach for storage, sharing and retrieval of encrypted data in the cloud. IEEE Access 170101–170116 (2020)
12. Dou, H., et al.: Dynamic searchable symmetric encryption with strong security and robustness. IEEE Trans. Inf. Forensics Secur. **19**, 2370–2384 (2024)
13. Yang, X., Lu, R., Choo, K., Yin, F., Tang, X.: Achieving efficient and privacy-preserving cross-domain big data deduplication in cloud. IEEE Trans. Big Data **8**(1), 73–84 (2022)
14. Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., Xiang, Y.: Block design-based key agreement for group data sharing in cloud computing. IEEE Trans. Depend. Secure Comput. **6**(6), 996–1010 (2019)
15. Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., Chen, D.: Enhancing cloud-based IoT security through trustworthy cloud service: an integration of security and reputation approach. IEEE Access **7**, 9368–9383 (2019)
16. Suwansrikham, P., She, K.: Asymmetric secure storage scheme for big data on multiple cloud providers. In: IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, pp. 121–125 (2018)
17. Halabi, T., Bellaiche, M.: Towards security-based formation of cloud federations: a game theoretical approach. IEEE Trans. Cloud Comput. 928–942 (2018)
18. El-Booz, S., Attiya, G., El-Fishawy, N.: A secure cloud storage system combining time-based one time password and automatic blocker protocol. In: 11th International Computer Engineering Conference (ICENCO), pp. 188–194 (2015)
19. Gai, K., Qiu, M., Zhao, H.: Security-aware efficient mass distributed storage approach for cloud systems in big data. In: IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 140–145 (2016)