electronics

MDPI

Article

Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments

Reyana A [1], Sandeep Kautish [2], Sapna Juneja [3], Khalid Mohiuddin [4], Faten Khalid Karim [5], Hela Elmannai [6,*], Sara Ghorashi [5] and Yasir Hamid [7]

[1] Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore 641114, India
[2] Department of Computer Science and Engineering, Lord Buddha Education Foundation, Kathmandu 44600, Nepal
[3] Department of Computer Science, KIET Group of Institutions, Delhi NCR, Ghaziabad 201206, India
[4] Department of Management Information Systems, College of Business, King Khalid University, Abha 62529, Saudi Arabia
[5] Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[6] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[7] Information Security Engineering Technology, Abu Dhabi Polytechnic, Abu Dhabi 111499, United Arab Emirates
* Correspondence: hselmannai@pnu.edu.sa

Abstract: With the growing number of cloud users, shared data auditing is becoming increasingly important. However, these schemes have issues with the certificate management. Although there is a certificate-shared auditing scheme, it is ineffective in dealing with dynamic data and protecting data privacy. The verifier cannot access the data content to ensure data integrity due to security concerns. This paper proposes a novel technique to ensure the integrity and improve the access control. A novel enhanced storage retrieval mechanism is used to improve the performance of the cloud's storage and retrieval mechanisms to achieve this. The technique is evaluated in concern of the upload, download, encryption, and decryption time. As the file size grows, so does the time it takes to upload it. Similarly, the time taken to encrypt files of various formats and sizes evidenced that it depends on the file size and format. Thus, the encryption time increases as the file sizes increases, demonstrating the performance of the proposed system.

Keywords: cloud computing; security; encryption; decryption; blockchain

Citation: A, R.; Kautish, S.; Juneja, S.; Mohiuddin, K.; Karim, F.K.; Elmannai, H.; Ghorashi, S.; Hamid, Y. Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments. *Electronics* **2023**, *12*, 714. https://doi.org/10.3390/electronics12030714

Academic Editors: Celestine Iwendi, Thippa Reddy Gadekallu and Bahman Javadi

Received: 2 January 2023
Revised: 18 January 2023
Accepted: 25 January 2023
Published: 1 February 2023

1. Introduction

Today, the process of cyber-physical systems incorporates both processing and data transmission. The significant challenge here is the legal and ethical perspective. Hence, for these systems, data security needs to be addressed. Recently, researchers have been interested in global cyber-physical systems. As per the US National Science Foundation (NSF) report, sensing, computations, and networking are involved [1]. As the number of cloud users increases, data sharing grows, and data auditing becomes crucial. To address this issue, various public key infrastructure-based techniques are applied. Despite this, there exists the issue of certificate management. Although a certificate-shared auditing scheme was proposed, it is inefficient in handling dynamic data and protecting data privacy. Due to security, the verifier cannot access the information and ensure its integrity. With the rise of cloud services, storage services are provided without human interaction [2]. Therefore, ensuring data integrity is vital. In the case of cloud users they download thinking integrity is maintained [3]. When a member of the group uploads a file, other members can access and modify it. Applications such as Dropbox are used in many companies for employees

to work together. Whereas the cloud service provider (CSP) ensures data integrity. The possibility of data corruption exists due to hardware or software failure. Hence, the integrity of stored data applies RDPC schemes to generate an authentication tag for each block. The status of the data is verified by the correctness of the tag. In block updating, the regeneration of the tag is another challenge. They generate the authentication tags while auditing, which increases the checking complexity. Additionally, the group is dynamic, so the user revocation must be addressed. Those who revoke all their public/private keys are to be made invalid [3]. Cloud computing benefits the user in terms of scalability, cost, and ease of access. A massive amount of cloud providers are finding difficulties in handling malicious attackers [4]. This paper proposes a novel framework to safeguard the integrity of the data and ensure user access. To accomplish this, the contributions involved are as follows: A security-enhanced cloud storage and retrieval mechanism (ECRM) to improve the storage and retrieval mechanisms for cloud users. To evaluate the performance of the proposed ECRM through various metrics and show its effectiveness in the cloud environment. To carry out the analysis in terms of the upload, download, encryption, and decryption times by varying the file size and formats. Finally, the performance of the proposed technique is compared with the existing model [5]. The rest of the article is organized as follows: Section 2 gives a review of the various literature studies; Section 3 expands on the proposed methodology, and Sections 4 and 5 discuss the results and conclusion.

2. Related Works

They surveyed the various blockchain applications [6] used for communication, sensing, and computation. Experts also proposed a mathematical formulation for analyzing the use of distributed ledger techniques. According to the authors, the use of the blockchain will validate the transactions. However, ensuring user privacy and authentication remains challenging. The authors of [1] described the incorporation of a cyber-physical data transmission process. The legal and ethical implications of privacy continue to be a source of contention. The authors presented a blockchain-based intrusion detection model for data transmission. The model's stages are acquisition, intrusion detection, encryption, transmission, and classification. To detect anomalies, the model employs a deep belief network and secures the transmission via a blockchain. The residual network is used for subsequent classification. For intrusion detection, the model made use of the NSL-KDD 2015 dataset. Although the detection anomaly rate is 98.95% and the classification accuracy is 98.45%, the model was only appropriate for healthcare. Other applications, on the other hand, remain a challenge. In [5], the experts utilized cloud services and proposed a scheme to support the simultaneous updates of multiple data blocks. Thus, overcoming the efficiency limitation. The scheme employed an erasure-coded hierarchical log structure to support the delayed update of multiple blocks and data retrievability. In addition, homomorphic tags are used to reduce the amount of data transmissions and enhance the efficiency of data updates. Although, the results of their scheme evidenced that the computation cost was high. The rapid adoption of information technology has accelerated the use of data storage. The use of the cloud has accelerated this growth, but it has limitations in terms of privacy and security. The verification of the integrity using public key infrastructure has increased the security risk and computation cost. The authors of [7] created an integrity auditing method that makes use of Shamir's secret key sharing. This entails the distribution and administration of secret keys. As a result, the platform is secure and reliable. Although this method is efficient, if a manager fails to decrypt it, the threshold must be reset. A hybrid algorithm proposed by [8] makes use of an encryption algorithm. It combines homographic and blowfish encryption to improve cloud security. Although the technique provided data confidentiality, the authors emphasize the need for other algorithms to address the security issues that large firms face when using cloud storage. For a multi-dimensional (t, n) threshold quantum state sharing scheme is proposed. The transformed secret state is shared by the multi-coin quantum walk. The identity of the participant and validation of the secret is verified with the help of the rotational unitary operator and the hash func-

tion. The correctness of the proposed protocol is proved by a determined case and an experimental simulation result performed on the IBM Quantum Experience. This can be applied to online e-government and e-business systems. Experts behind [9] created a tool for distributing data across multiple clouds. Each user file is encrypted using a block-based data encryption algorithm, so the field must shuffle the data bytes [10]. These data are nonlinearly distributed across multiple clouds after being shuffled and encrypted. The file contents are protected using this method, and no service provider can understand them. The experts behind [11] proposed a framework for uploading data, slicing, encrypting, and distributing it, then decrypting, retrieving, and combining it. The algorithm was designed to secure big data before it was stored in the cloud. For the simulation, a real-time cloud environment was used, and the encryption process recorded 2630 KB/s. Despite being recorded, the algorithm's efficiency was only 53.8%. Using the Diffie–Hellman protocol, [12] proposed a cloud storage auditing mechanism (PP-CSA scheme) for data sharing. From the experimental results, it is demonstrated that the algorithm achieves a desirable level of efficiency with the use of a blockchain-based smart grid access control system [13]. The authors used a decentralized blockchain for smart grid access control. The meters are registered offline, and the meter authenticates the associated service [14]. The secret key-securing pairwise consensus procedure takes the highest computation time as the number of transactions considered is higher [15]. Although the scheme provides improved security, achieving lower computation costs remains a challenge. The authors proposed a jointly connected network model [16], in which the CPS can be represented at various times while connecting the graphs. To formulate the detection of collaborative events, the consensus problem is used. The performance was assessed, and it is observed that the node can iteratively calculate the neighboring active node, improving reliability and scalability. However, significant reductions in computation costs remain a challenge. A public auditing system ensures [17] data privacy for cloud data. The system supports batch and dynamic auditing. The authors protected the system from unauthorized access using an automatic blocker protocol. Although the system is extremely secure and effective, future efforts concerning the multi-cloud environment remain a challenge.

3. Materials and Methods

Cloud service providers allow scalable storage services [18]. Where one of the user's private keys is considered as an authentication for the public auditing solution. The data's integrity is checked using the public key of each block. Privacy concerns are a challenge in such models [19]. This paper proposes a novel ECRM framework to ensure data integrity and user access control. The method improves efficiency during data storage and retrieval in the cloud as shown in Algorithms 1 and 2. The proposed security model's framework is depicted in Figure 1.

In Figure 1, the system initially identifies the group leader and members for data storage and retrieval. The group head is in charge of the group and has access to user allocation, revocation, and user access count control [20–23]. The group head will be communicated to join the group to access the cloud data. The head grants them to an authorized user, and each user is given a key and a digital signature [24]. The auditing database maintains the secret key. The user is granted cloud access after obtaining the digital signature and verifying it [25]. The data accessed will be saved in the cloud in the appropriate formats for later retrieval. Data integrity is maintained by granting access to data only after it has been decrypted [26]. The auditing team verifies these further. By ensuring data integrity, the model emphasizes cloud security [27,28]. The provided digital signature is used to control user access and revocation. When a user revokes an attribute, it is converted to a null value, thus preventing cloud access in the future [29]. The data owner identifies the user Un, as shown in Equation (1), where the encryption [30,31] is performed using the random value Zp [32,33]. Here, *DN* is the data name, *EX* is the extension, and *MS* is the memory space, as expressed in Equation (2).

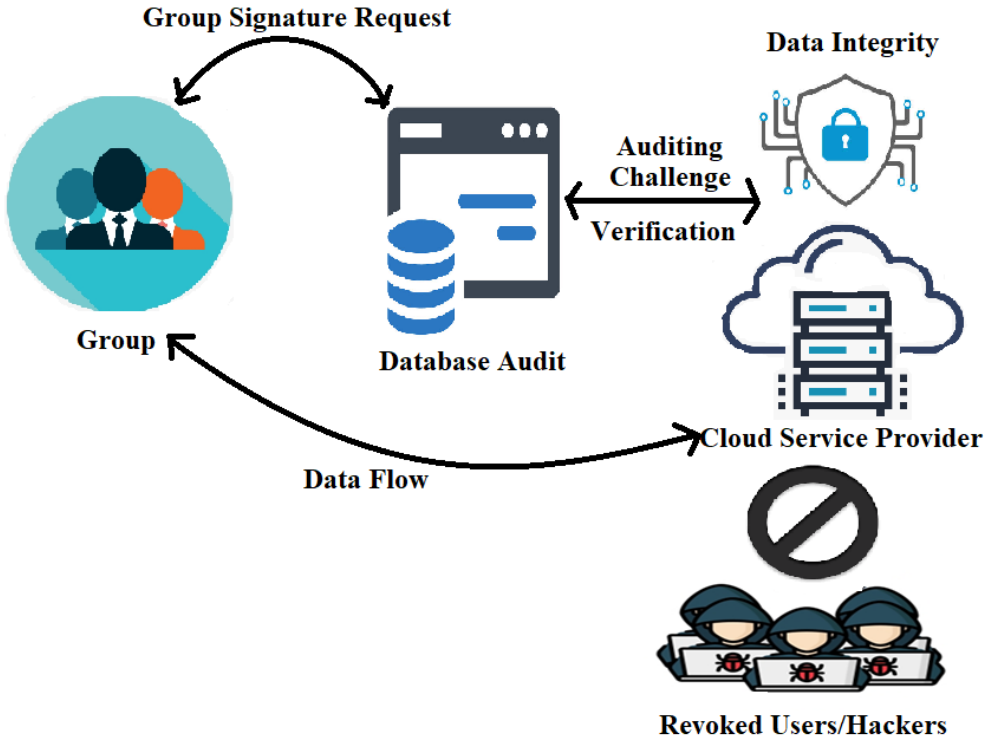

Figure 1. Proposed ECRM framework.

$$CT_E = m^y \ mod \ n \tag{1}$$

$$SCT_E = \left(T', \ CT_E, \ DN, \ EX\right) \tag{2}$$

Cloud storage of encrypted cipher text. The retrieval and decryption are represented by Equations (3) and (4).

$$RCT_E = CT_E\left(T', \ Q\right) \tag{3}$$

$$m = CT_E^d \ mod \ n \tag{4}$$

Algorithm 1 Encryption

1: begin
2: Encrypt(*UK*, *M*, *n*, *e*, *DS*, *IDU*, *RID*, *Km*, *Kp*)
3: $CT_E \leftarrow$ *UK* (*f*(*M*, *n*, *e*))
4: for $i \leftarrow 1$ to n do
5: if [*DSi*, *IDUi*, *RIDi*] == [1, 1, 1] then;
6: $Ks \leftarrow Km \oplus Kp$;
7: Add *Ks* user;
8: Upload CT_E;
9: else
10: Deny;
11: end for
12: Delete *Km*, *Ks*;
13: end
14: $MS \leftarrow (T', C, DN, EX)$
15: end

Algorithm 2 Decryption

1: begin
2: Decrypt (K_s, Q Kp, UK, CT_E, n, d, DN, T_u)
3: If K_s == 1 then;
4: for each user i, do
5: $Km \leftarrow K_s \oplus Kp$;
6: $M \leftarrow UK(f(CT_E, n, d))$;
7: end for
8: else
9: return;
10: end If
11: for $u \leftarrow 1$ to T do
12: if $DN \in Q$ then
13: $CT_E(T', Q) \leftarrow 1$;
14: else
15: $C(T', Q) \leftarrow 0$;
16: end if
17: end for
18: if $CT_E(T', Q) == 1$ then;
19: C associated with T' to the user U_i
in response
20: end if
21: end

4. Results

The experiments were conducted using an Intel I3 processor with 4 GB RAM and the Win10 operating system. To evaluate the efficacy of the scheme, the Eclipse platform and Java Pairing-Based Cryptography (JPBC) were used to perform cryptographic operations. The proposed ECRM framework's performance was evaluated using the metrics upload, download, encryption, and decryption time. The upload time is the amount of time it takes to store a file in the cloud. The download time is the time taken for retrieval. The time required was calculated using the various file sizes for various file extensions. The two types of file extensions considered in this study are .txt and .jpg. For technical feasibility, the file sizes considered range from 10 KB to 30 MB.

Figure 2 shows an analysis of the upload time (UT) in milliseconds for file sizes of 10 kb, 30 kb, 50 kb, 70 kb, 90 kb, 2 Mb, 15 Mb, and 30 Mb, with an upload time in milliseconds of 1, 1, 2, 2, 3, 4, 5, and 6, respectively. As the file size increases, so does the time it takes to upload it. However, there is no significant difference in the uploading times of a 10 KB file of 1 (ms) and a 30 MB file of 6 (ms), thus demonstrating the performance of the proposed system.

Figure 3 depicts a download time (DT) analysis in milliseconds for file sizes of 10 kb, 30 kb, 50 kb, 70 kb, 90 kb, 2 Mb, 15 Mb, and 35 Mb, with download times of 897 (ms), 897 (ms), 1067 (ms), 1115 (ms), 1115 (ms), 1781 (ms), 1958 (ms), and 2045 (ms), respectively. The time it takes to upload a file rises in proportion to its size. It was discovered from the output that both times increase as the data size increases. For the same file sizes, the values were found to be nearly equal, thus demonstrating the performance of the proposed system.

Figure 4 shows an analysis of the encryption time (EnT) in milliseconds for file sizes of 10 kb, 30 kb, 50 kb, 70 kb, 90 kb, 2 Mb, 15 Mb, and 35 Mb, for 43, 74, 95, 115, 127, 145, 166, and 234 milliseconds, respectively. The time taken for encryption depends on the file size and format. The encryption time increased as the file sizes increased. Similarly, the decryption time (DeT) is shown in Figure 5.

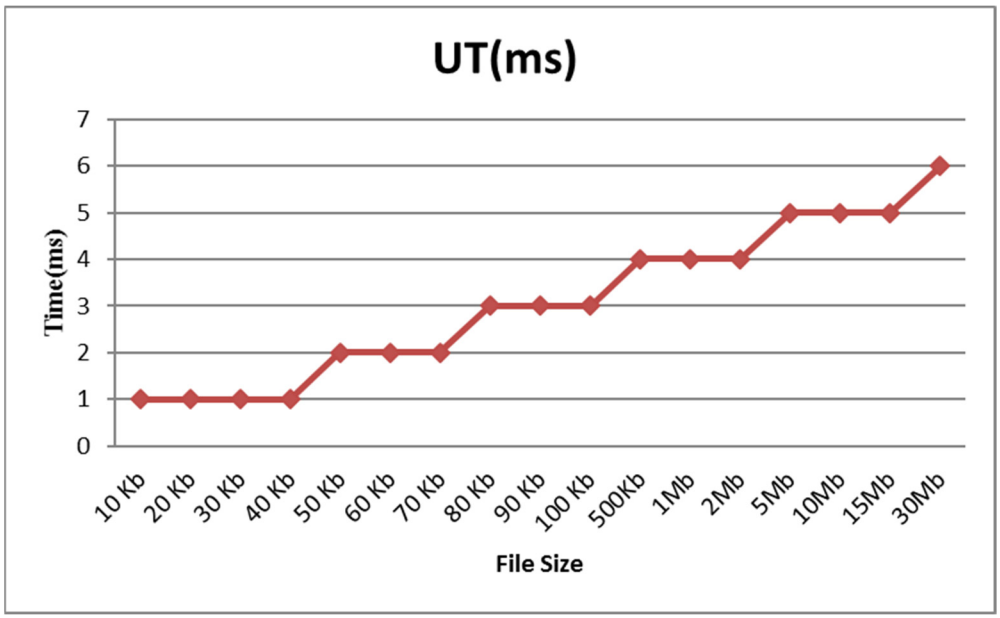

Figure 2. Upload time.

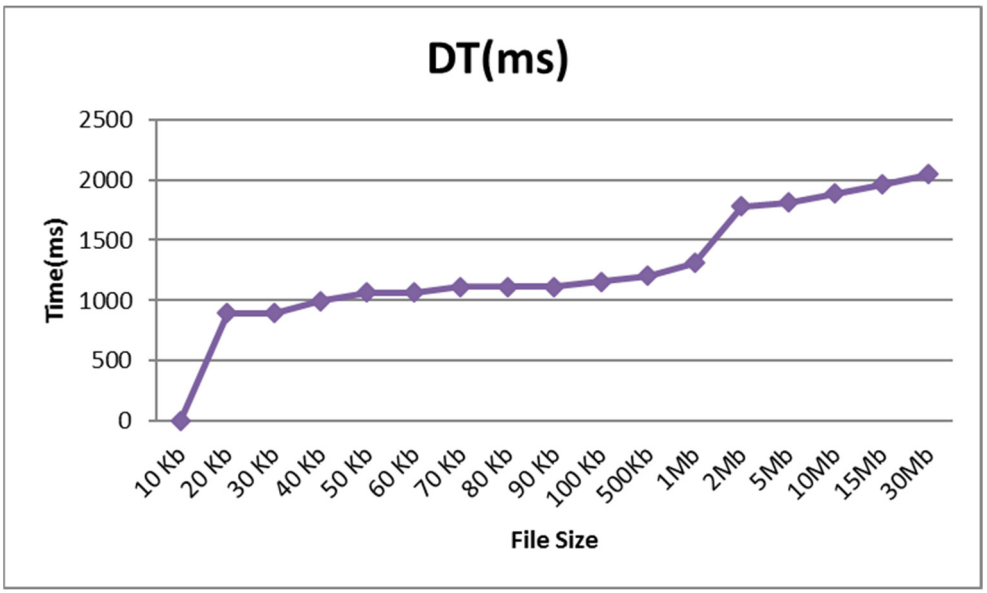

Figure 3. Download time.

Concerning the group user, the efficiency of the proposed techniques varies. Additionally, the number of blocks per file is assumed to be similar to IPIC-DG. The proposed technique shows better efficiency when compared to other schemes. In comparison to the existing technique [5], for the proposed technique, the communication cost is smaller, as each user file is cMulExpG1. However, the communication cost remains a challenge as it is the constant, as *clq* + *cls*, for all techniques as shown in Table 1. Thus, if a file transmission attempts to decrypt using a false key, the user who entered the incorrect key will be revoked. When using a safe file, the signature must be original, and the decryption must match the same. Thus, for database verification, effective updates are vital to achieving efficient and secure data integrity auditing for shared dynamic data in a multi-user environment.

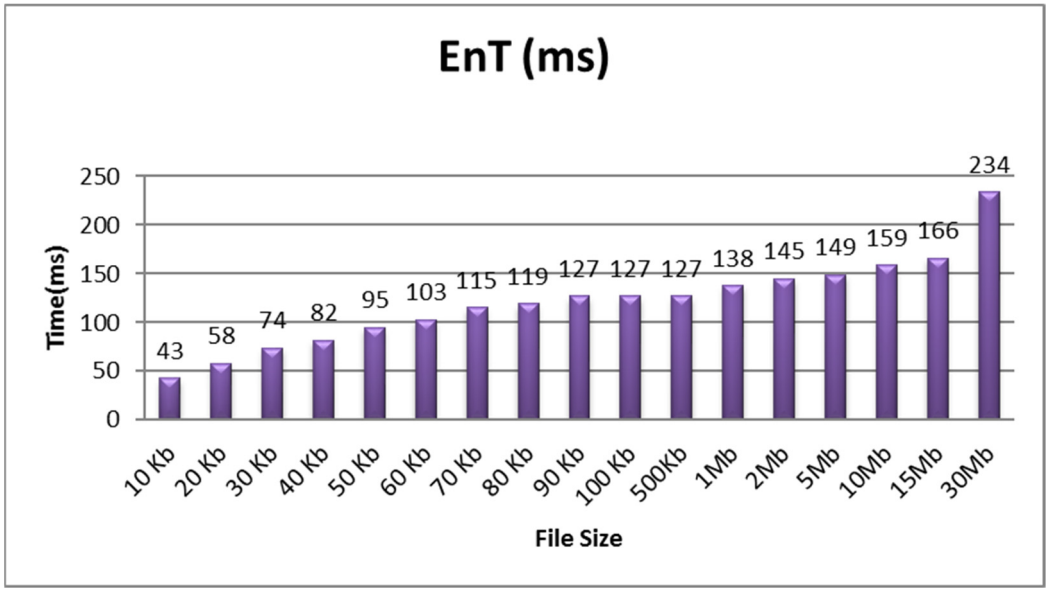

Figure 4. Encryption time.

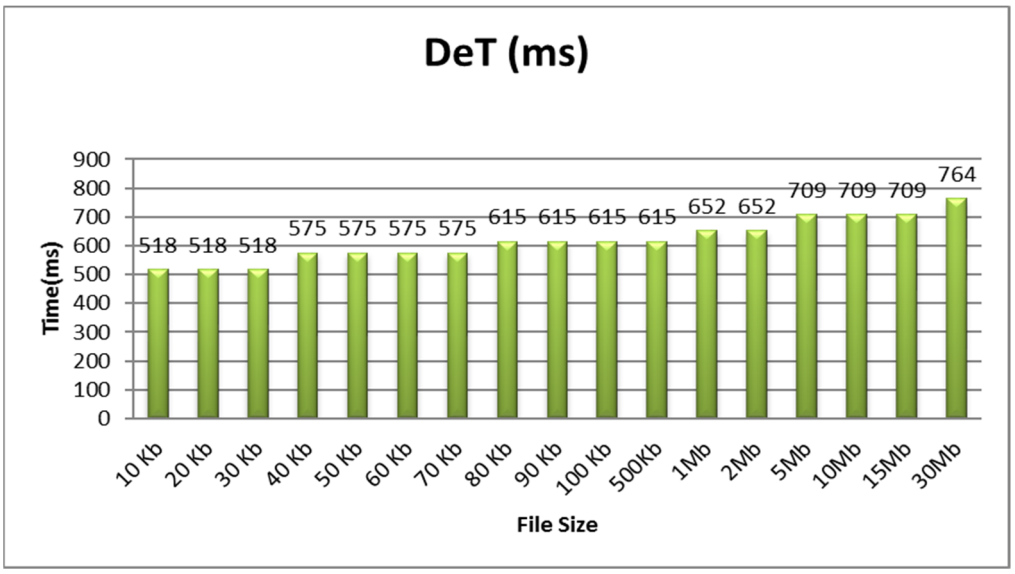

Figure 5. Decryption time.

Table 1. Comparison of the proposed with the existing scheme.

Parameters	Existing [5]	Proposed—ECRM	Existing [22]
Signature Efficiency	$((4+m)z+4) \times MulExp_{G_1}$ $+zMulExp_{G_T} + 3Pair$	$(4mz) * zMulExp_{G_1}$ $+zMulExp_{G_T} + mPair$	$O(\lambda\beta \log 2\ n)$
Computation Cost	$(c+3)MulExp_{G_1} + cMulExp_{G_T} + 2Pair$	$cMulExp_{G1}$	$O(\beta)$
	$cl_q + cl_s$	$cl_q + cl_s$	$O(\beta \log n)$
	$ml_q + l_{name} + (m+1)l_{G_1}$	$m(l_q + l_{name} + l_{G1})$	$\beta \log n + O(\lambda \log n)$

where z -> the number of blocks allotted for a file; m -> group user; Exp_{G1} -> exponent in the group; c -> the number of selected blocks; lq -> the length of elements on $\mathbb{Z}^*q$; ls -> the length of the challenge index; $Pair$ -> bilinear pair; Mul -> multiplication; S -> a number of challengers or users; β -> block size; λ -> the security parameter; and n -> an upper bound on the number of blocks.

5. Conclusions

The ECRM mechanism proposed in this paper ensures data integrity by improving user accessibility control. The results show that the proposed technique demonstrates data-sharing efficiency. It encrypts, preventing privacy leakage and security attacks, and

audits the data while downloading, thus ensuring data integrity. The encryption time was calculated for files of various formats and sizes, and it was discovered that the encryption time varied depending on the size and format of the files. As the file sizes increased, so did the encryption time. The evidence shows that communication costs vary and that the proposed system is very simple, demonstrating its performance.

Author Contributions: Conceptualization S.K. and R.A.; methodology, S.G.; software, R.A.; validation, S.J. and Y.H.; formal analysis, Y.H. and K.M.; investigation, R.A. and S.K.; resources, H.E.; data curation, S.K.; writing—original draft preparation, R.A., S.J. and S.K.; writing—review and editing, S.K., YH. and F.K.K.; visualization, H.E. and S.G.; supervision, S.K. and S.J.; project administration, S.K., S.J. and Y.H.; funding acquisition, H.E., F.K.K. and S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research project was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R300), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: All the data are available within the article.

Acknowledgments: This research project was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R300), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel Distrib. Comput.* **2021**, *153*, 150–160. [CrossRef]
2. Mante, R.V.; Bajad, N.R. A study of searchable and auditable attribute based encryption in cloud. In Proceedings of the 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 10–12 June 2020; IEEE: Piscataway, NJ, USA, 2021; pp. 1411–1415.
3. Vennala, A.; Radha, M.; Rohini, M.; Anees Fathima, M.; Lakshmi, P.D. Efficient Privacy-Preserving Certificateless Public Auditing of Data in Cloud Storage. *J. Eng. Sci.* **2022**, *13*, 532–541.
4. Li, R.; Yang, H.; Wang, X.A.; Yi, Z.; Niu, K. Improved Public Auditing System of Cloud Storage Based on BLS Signature. *Secur. Commun. Netw.* **2022**, *2022*, 6800216. [CrossRef]
5. He, J.; Zhang, Z.; Li, M.; Zhu, L.; Hu, J. Provable data integrity of cloud storage service with enhanced security in the internet of things. *IEEE Access* **2018**, *7*, 6226–6239. [CrossRef]
6. Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain-enabled cyber-physical systems. *Sensors* **2020**, *20*, 282. [CrossRef]
7. Chen, Y.; Liu, H.; Wang, B.; Sonompil, B.; Ping, Y.; Zhang, Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comput.* **2021**, *10*, 3. [CrossRef]
8. Sajay, K.R.; Babu, S.S.; Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–10. [CrossRef]
9. Latha, K.; Sheela, T. Block based data security and data distribution on multi cloud environment. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–7. [CrossRef]
10. Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-empowered cloud architecture based on secret sharing for smart city. *J. Inf. Secur. Appl.* **2021**, *57*, 102686. [CrossRef]
11. Viswanath, G.; Krishna, P.V. Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evol. Intell.* **2021**, *14*, 691–698. [CrossRef]
12. Xu, Y.; Ding, L.; Cui, J.; Zhong, H.; Yu, J. PP-CSA: A privacy-preserving cloud storage auditing scheme for data sharing. *IEEE Syst. J.* **2020**, *15*, 3730–3739. [CrossRef]
13. Bera, B.; Saha, S.; Das, A.K.; Vasilakos, A.V. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. *IEEE Internet Things J.* **2020**, *8*, 5744–5761. [CrossRef]
14. Liu, Z.; Wu, Z.; Gan, C.; Zhu, L.; Han, S. Datamix: Efficient privacy-preserving edge-cloud inference. In Proceedings of the Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, 23–28 August 2020.
15. Gudeme, J.R.; Pasupuleti, S.; Kandukuri, R. Certificateless privacy preserving public auditing for dynamic shared data with group user revocation in cloud storage. *J. Parallel Distrib. Comput.* **2021**, *156*, 163–175. [CrossRef]
16. Li, S.; Zhao, S.; Yang, P.; Andriotis, P.; Xu, L.; Sun, Q. Distributed consensus algorithm for events detection in cyber-physical systems. *IEEE Internet Things J.* **2019**, *6*, 2299–2308. [CrossRef]
17. Jalil, B.A.; Hasan, T.M.; Mahmood, G.S.; Abed, H.N. A secure and efficient public auditing system of cloud storage based on BLS signature and automatic blocker protocol. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 4008–4021. [CrossRef]

18. Liu, Q.; Wang, G.; Wu, J. An efficient privacy preserving keyword search scheme in cloud computing. In Proceedings of the 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009.
19. Babu, G. Secure Data Sharing and Identity Based Integrity Auditing with Hiding Privacy Information in Cloud. *Cikitusi J. Multidiscip. Res.* **2019**, *6*, 91–96.
20. Ma, H.; Zhang, Z. A new private information encryption method in internet of things under cloud computing environment. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8810987. [CrossRef]
21. Ram Prashath, R.; Srineeladevi, K. Inspecting Cloud Storage System for Secure Data Forwarding Using Advanced Encryption Standard. *Int. J. Res. Appl. Sci. Eng. Technol.* **2022**, *10*, 110–112.
22. Shi, E.; Stefanov, E.; Papamanthou, C. Practical dynamic proofs of retrievability. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin Germany, 4–8 November 2013; pp. 325–336.
23. Wang, Y.; Lou, X.; Fan, Z.; Wang, S.; Huang, G. Verifiable Multi-Dimensional (t, n) Threshold Quantum Secret Sharing Based on Quantum Walk. *Int. J. Theor. Phys.* **2022**, *61*, 24. [CrossRef]
24. Dhiman, G.; Rashid, J.; Kim, J.; Viriyasitavat, W.; Gulati, K. Privacy for healthcare data using the byzantine consensus method. *IETE J. Res.* **2022**, 1–12. [CrossRef]
25. Mittal, S.; Bansal, A.; Gupta, D.; Turabieh, H.; Elarabawy, M.M.; Bitsue, Z.K. Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health. *Comput. Intell. Neurosci.* **2022**, *2022*, 7016554. [CrossRef] [PubMed]
26. Uppal, M.; Gupta, D.; Juneja, S.; Sulaiman, A.; Rajab, K.; Rajab, A.; Elmagzoub, M.A.; Shaikh, A. Cloud-Based Fault Prediction for Real-Time Monitoring of Sensor Data in Hospital Environment Using Machine Learning. *Sustainability* **2022**, *14*, 11667. [CrossRef]
27. Singamaneni, K.K.; Muhammad, G.; Al Qahtani, S.A.; Zaki, J. A novel QKD approach to enhance IIOT privacy and computational knacks. *Sensors* **2022**, *22*, 6741. [CrossRef]
28. Juneja, S.; Juneja, A.; Bali, V.; Upadhyay, H. Cyber Security: An Approach to Secure IoT from Cyber Attacks Using Deep Learning. In *Industry 4.0, AI, and Data Science*; CRC Press: Boca Raton, FL, USA, 2021; pp. 135–146.
29. Singamaneni, K.K.; Nauman, A.; Viriyasitavat, W.; Hamid, Y.; Anajemba, J.H. An Efficient Hybrid QHCP-ABE Model to Improve Cloud Data Integrity and Confidentiality. *Electronics* **2022**, *11*, 3510. [CrossRef]
30. Uppal, M.; Gupta, D.; Mahmoud, A.; Elmagzoub, M.A.; Sulaiman, A.; Reshan, M.S.A.; Juneja, S. Fault Prediction Recommender Model for IoT Enabled Sensors Based Workplace. *Sustainability* **2023**, *15*, 1060. [CrossRef]
31. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2326–2341. [CrossRef]
32. Alazab, M.; RM, S.P.; Parimala, M.; Maddikunta, P.K.R.; Gadekallu, T.R.; Pham, Q.V. Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3501–3509. [CrossRef]
33. Wang, T.; Yang, Q.; Shen, X.; Gadekallu, T.R.; Wang, W.; Dev, K. A privacy-enhanced retrieval technology for the cloud-assisted internet of things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4981–4989. [CrossRef]