engineering proceedings

MDPI

Proceeding Paper

An Efficient and Robust Method for Data Privacy and Security on a Public Cloud Using a Novel Hybrid Technique [†]

Niroshini Infantia Henry [1,*], Chinnasamy Anbuananth [1] and Subramanium Kalarani [2,*]

[1] Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram 608002, India; anbu_ananth2006@yahoo.com

[2] Department of Information Technology, St.Joseph's Institute of Technology, Chennai 600119, India

[*] Correspondence: niroshini.siddarth@gmail.com (N.I.H.); kala.rani1971@gmail.com (S.K.)

[†] Presented at the International Conference on Recent Advances on Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: The end user has a cost-effective and cloud-based method of storing and retrieving their personal information through remote access using some kind of network connectivity. The user may view the data at any time and from any location they want. However, the data that are stored on the cloud may not always stay in a safe state. As the data can only be accessed by the end user via the intervention of a third party, the authenticity and integrity of the data are at risk of being compromised. It is possible for many people to utilize different Web access at the same time to access and recover their information stored on the cloud. As a consequence, a user's sensitive data are exposed, leaked, or lost in several locations. Cryptographic methods, such as the Elliptic Curve Cryptography, have been used in the development of a great deal of different algorithms and protocols, all with the intention of preserving the confidentiality and authenticity of the data (ECC). In this research, we present a safe and efficient method for exchanging data via the cloud, while simultaneously preserving both the data's security and their integrity. The suggested system primarily operates by combining the Elliptic Curve Cryptography (ECC) technique with the Advanced Encryption Standard (AES) method to guarantee verification and maintain the solidarity of data. The findings of the experiments demonstrate that the strategy that was presented is effective and produces superior outcomes when compared to other ways that are already in use.

Keywords: cloud computing; data security; authentication; data integrity; ECC; data privacy; AES

check for updates

Citation: Infantia Henry, N.; Anbuananth, C.; Kalarani, S. An Efficient and Robust Method for Data Privacy and Security on a Public Cloud Using a Novel Hybrid Technique. *Eng. Proc.* **2023**, *59*, 115. https://doi.org/10.3390/engproc2023059115

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 25 December 2023

1. Introduction

Cloud computing has been acknowledged for its role in generating a range of novel user groups and marketplaces within the realm of information technology in recent times [1]. Cloud computing services are provided to customers through data centers located in various geographic locations worldwide. Cloud computing is one of a number of significant computing paradigms that provides a wide range of features that may be accessed from any region and on any device. These services include limitless database storage, networks and communications, and a variety of other options. Due to its appealing characteristics, there is an ever-increasing dependence on the cloud, which has resulted in an enormous amount of data and raised worries over both privacy and security [2]. The utilization of cloud services by individuals can potentially give rise to substantial issues pertaining to cloud computing, specifically with respect to the security of data and occurrences of data breaches. Due to this, unauthenticated and unauthorized sources need to have their data access privileges severely curtailed. In the event that client users are allowed to reassess APIs and data, this might lead to data breaches and the resulting loss of information. Therefore, cryptographic methods are primarily used to safeguard the data that are stored on the cloud. This is accomplished by using encryption/decryption procedures with the assistance of a variety of keys. Asymmetric key encryption is another name for public key cryptography, which uses both public and private keys to encrypt and decrypt communication. These keys are included inside the file. In addition, symmetric key encryption is used to safeguard the information. Encryption and decryption are performed using a unique secret key for this kind of encryption. Encrypting the communication using the private key helps protect it from being read by any of the hackers who may be active. The difficulty in implementing symmetric cryptographic methods is due to the length of the key needing to be sufficiently large to provide adequate protection [3]. The challenge in implementing symmetric cryptographic methods has been traced back to this need. The primary objective of the Data Encryption Standard (DES) was to eventually be succeeded by the Advanced Encryption Standard (AES), which utilizes the symmetric key encryption methodology. With a 128-bit key length, AES is substantially faster than DES. The Data Encryption Standard (DES) utilizes a key length of 64 bits. In contrast to prevailing frameworks, the Elliptic Curve Cryptography (ECC) employs asymmetric key encryption, which confers a significant advantage of enhanced security with a reduced key size compared to other established systems like the Rivest–Shamir–Adleman(RSA) method. The RSA method relies on symmetric cryptography, leading to decreased latency and computational requirements. Chen et al. suggested using AES in conjunction with ECC, and they really did utilize AES in conjunction with ECC in order to make the system more secure. In addition to that, they made use of the Shamir secret sharing key in order to send the data. In this piece of research, we advocated the use of a hybrid architecture that combines AES and ECC to ensure the safety of the data stored on the cloud without the need for any external party. The suggested hybrid paradigm, known as AES-ECC, is used in order to effectively keep the system's security intact while using cloud storage. The primary advantage of using a hybrid strategy is the time and space savings that can be realized while still preserving the integrity of the information stored on the system. Despite the availability of a large number of authentication techniques, neither the time nor the cost of computing have significantly decreased. Computing on the cloud is an exciting new technology that has the potential to assist businesses in growing their operations and securely moving information from their current locations to a server in the "cloud" that can be retrieved at any moment and from any place. The many features of cloud computing allow for various services to be provided to users, regardless of the sort of user they are, However, these services are dependent on the users' work [4]. The majority of the services that may be obtained using cloud computing are shown in Figure 1.

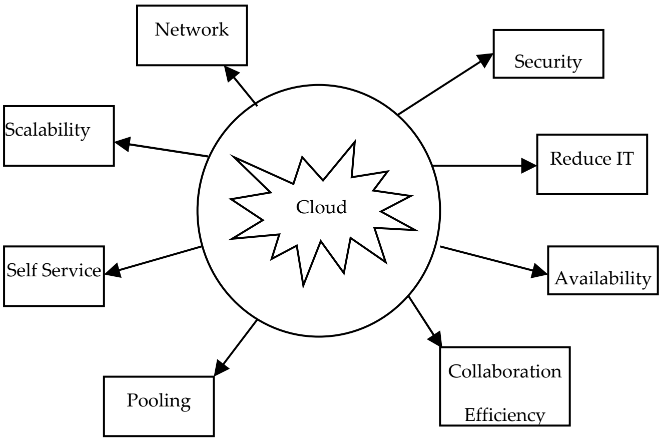

Figure 1. Various services in cloud.

Online storage users can now take advantage of a variety of services, including those that enable incredible content encryption and decryption without the help of a third party. This enhances the platform so that information may be recovered rapidly and safely in a secure setting while also increasing the system's reliability and storage effectiveness.

Through the use of this service, various categories of users are able to effortlessly share cloud resources. This service also helps to improve the capabilities of the system by ensuring the safety of additional storage space following the use of cryptographic methods [5]. Figure 2 illustrates the many types of cloud storage services now available. The data exchanged between the receiver and sender are protected, decoded, and kept on the remote server may be seen clearly. In addition to this, it denotes the safe transfer of data via the use of cloud storage.

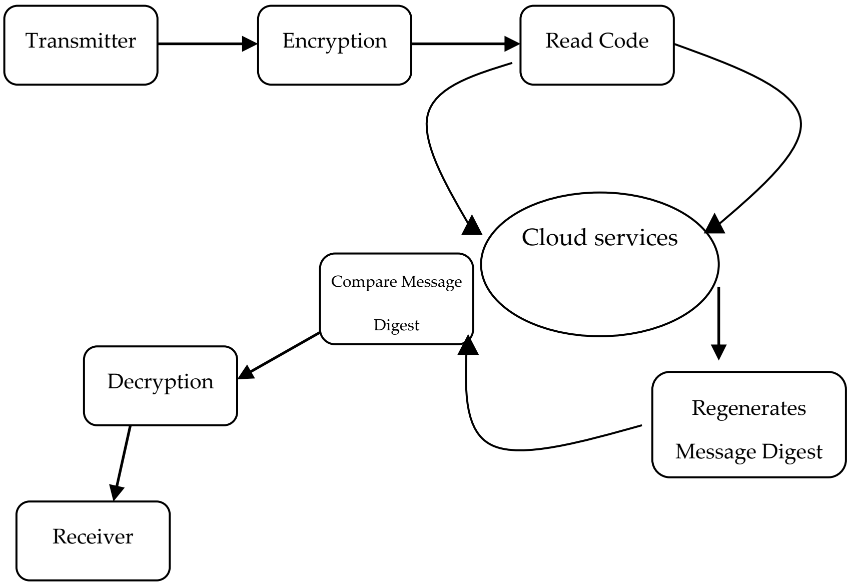

Figure 2. Cloud Storage Services.

AES and ECC are combined in a blended paradigm that we show. In our proposed methodology, we used ECC to help us generate the key pairs of AES. In other words, we are not making use of the key that was created with the AES method. Instead, we are making use of the ECC algorithm to generate the key in order to lower the key size. Both public and private keys may be used to secure and decode information, just as in asymmetric and symmetric encryption techniques. As a result, this procedure calls for a significant key length and a significant amount of processing time. The AES-ECC blended technique that was suggested is utilized to improve the system's security in a shorter amount of time by resolving the issue of key length. Additionally, it assists in lowering the amount of computing power required for memory optimization. It also provides an approach that explains how well the ECC approach is used to generate the key pair and how the AES algorithm is used to encrypt and decrypt data. Our proposed plan includes this technique.

2. Related Study

Cloud computing does have certain drawbacks, one of which is the security of the data that are stored, particularly with regard to the picture files that are susceptible to being readily modified. It is necessary to use both the AES cryptography and the LSB steganography technologies in order to increase the data security provided via the JPG file type when using cloud computing. The author of publication [6] designed an AES 128 algorithm cryptography procedure to confuse the messages that will be inserted and used LSB steganography to disguise the messages that were scrambled. Both of these processes are described in this study. StegSpy was used in order to perform the analysis on the data. According to the findings of this investigation, the Platform as a Service cloud computing service led to the production of ciphered text that was attached to JPG/JPEG pictures by making use of the Least Significant Bit (LSB). The encryption outcome tested on the JPG/JPEG files produced a file that was larger than the original file in five out of five instances. The size of JPG and JPEG files will increase according to the amount of characters that are included inside the added text.

The author in [7] presented a cloud-based architecture that would handle security vulnerabilities in the various data storage platforms that are now in use. Due to the conventional design and operations that are applied to current storage systems in Bahrain for the purpose of managing data, there are a variety of cyber security risks that may be poised to these systems. It was determined that moving Bahrain's local storage services to a cloud environment would resolve a large number of the country's connected cyber security challenges. On the other side, a number of cyber security vulnerabilities were revealed to have evolved as a consequence of this shift. Some examples of these vulnerabilities include exposure to public networks and shared infrastructure that is used by several tenants. The move itself introduces weaknesses, which in turn induce security breaches, which in turn pose a danger to the sensitive information that lies under the surface. It provides an in-depth analysis of the relevance of moving storage services to the cloud environment as well as the newly arising concerns around cyber security brought about by such a move. The purpose of the proposed framework is to provide support for the many security strategies currently in place for information systems. In addition to this, it grants specialists in the field of cyber security the capacity to develop and tailor cloud services so that they are more suitable for the requirements of enterprises. A crucial precondition for the operation of cloud-based systems is the provision of secure data transfer. This study focuses mostly on risk considerations that arise as a result of cloud data management and discusses potential solutions to these problems. The purpose of this study is to discuss a method of hybrid encryption that can preserve the privacy and security of cloud storage. The ECC and the AES are, respectively, the two finest asymmetric encryption algorithms and the greatest symmetric encryption technology. Both of these acronyms stand for Elliptic Curve Cryptosystem and Advanced Encryption Standard. The AES-ECC hybrid cryptosystem combines the advantages of the ECC algorithm, which is based on symmetrical session key exchange, with the benefits of the AES algorithm, which speeds up data encryption. The delay factor is reduced to a minimum using the suggested strategy, which is also computationally efficient, resilient, and trustworthy.

The transfer of data in a secure manner is one of the fundamental requirements of any cloud-based architecture. The author discusses a hybrid encryption strategy in the article by [8], which is intended to preserve cloud users' privacy and security. The Elliptic Curve Cryptosystem (ECC) and the Advanced Encryption Standard (AES) are, respectively, the greatest symmetric encryption technology and the best asymmetric encryption techniques. The AES-ECC hybrid cryptosystem combines the advantages of the ECC algorithm, which is based on symmetrical session key exchange, with the benefits of the AES algorithm, which speeds up data encryption. The suggested solution reduces the delay factor to the smallest possible value while simultaneously being computationally efficient, resilient, and secure. As a direct result of cloud-based computing raising popularity, a paradigm shift is taking place in the field of information technology. As a result of the parallel and adaptable services it provides, cloud computing is quickly becoming the go-to option not just for people but also for businesses of every size. To secure the data and the privacy of the vast majority of cloud users, serious security vulnerabilities that are now present in cloud computing need to be solved. To address the primary managerial challenge, the author in [9] proposed a hybrid approach to this issue. The information stored on the cloud is secured using AES encryption together with a private key. The ECC algorithm is then used to encrypt the 256-bit AES key. With the use of LSB steganography, the user's picture will have the ECC encrypted key hidden inside of it. If the user wants to share cloud data with another user, all he has to do is include the AES key in the picture that the second user uploads to the cloud. Thus, it will be able to obtain a high level of security by using steganography, ECC, and AES. This will allow for efficient key management and dissemination among various users.

The concept of cloud computing is new in the realm of commercial infrastructure, and it promises eliminate the need of managing and maintaining costly computer gear. The risk to data likewise increases in tandem with the development of the market. To protect data from being accessed without authorization and to verify that the data have not been tampered with, a plan has been developed that, in addition to resolving the issues of privacy and consistency, also addresses the issue of unauthorized access. The author of article [10] suggested a hybrid technique called PHECC (Polynomial-based Hashing and Elliptic Curve Cryptography). This approach combines PH with ECC security procedures in order to guarantee the customers that users' data will be secure while they are stored on the cloud. In the present environment, the hybrid algorithm provides an almost absolute assurance of data safety. The effectiveness of the suggested method is evaluated alongside that of several existing hybrid algorithms.

3. Methodology

A brief explanation of the research methodology used in the work is presented. In the following section, the study plan for the recommended method is explained in more detail. The research process is illustrated in Figure 3, which shows a typical flow from an analysis of the existing schemes to the presentation of a new one.

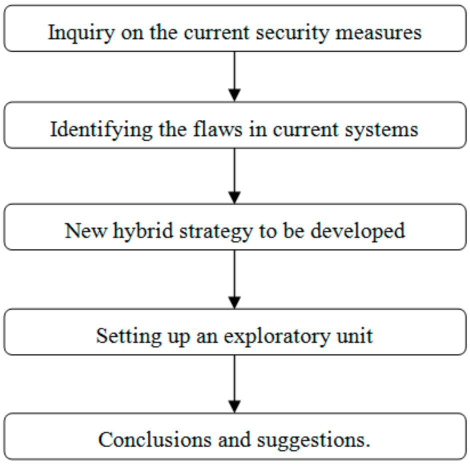
Inquiry on the current security measures
Identifying the flaws in current systems
New hybrid strategy to be developed
Setting up an exploratory unit
Conclusions and suggestions.

Figure 3. Suggested methodology.

3.1. ECC and AES

In order to prevent unwanted access to data, ECC utilizes an asymmetric key encryption method. A set of public and private keys is used to secure the ECC. ECC employs fields with only two dimensions, binary and prime numbers. ECC employs improved operations and provides a connection between binary and primary fields that cannot be accessed by unauthorized individuals; therefore, hacking is difficult when employing this cryptographic technology. ECC relies heavily on its small key size. The maximum number of points might be useful in locating the most acceptable field for implementing cryptography on data to enhance security. An initial selection is made, which then generates the huge number based on the data that ranges from zero to Z. The use of ECC to generate a key greatly simplifies the procedure. Due to its small key size, ECC offers a significant improvement over alternative cryptographic method. ECC methods are used in this study to improve memory and storage capacity. AES is one of the block cipher texts that employ AES. To protect the data, this method encrypts and decrypts it using a single key. It is the most popular algorithm used to strengthen regulations for cloud storage safety in cloud computing strategies. The AES technique is used in this research because it is easy to implement and works well with cloud computing and data storage. The only axis used in [9] is x. ECC encryption and decryption are demonstrated using Algorithms 1 and 2, respectively. Point addition, multiplication, and subtraction are the only operations that can be performed. The points produced by these point operations are located on the same curve as the one selected, i.e., P in Algorithms 1 and 2.

Algorithm 1: Encryption using ECC

```
Input: Elliptic curve attributes (P, e, E, b); private key $E_s$ and public key $E_u = E_sE$.
Output: Cipher text (DS1, DS2).
Ensure: Convert message AES key L to point on elliptic curve N.
Choose $h \in T^{[1,b-1]}$;
Evaluate DS1 = hE;
Evaluate $DS2 = N + hE_u$;
Return (DS1, DS2).
```

Algorithm 2: Decryption using ECC

```
Input: Elliptic curve Attributes (P, e, E, b); private key $E_s$ and cipher text ($DS_1$, $DS_2$).
Output: AES key H as message N.
Ensure:
Evaluate $N = DS_2$- $dDS_1$;
Extracting key H from N;
Return (H).
```

This information is decrypted using a private key, E_{sB}. It is important to note that the scalar and elliptic curve product satisfies the commutative property of multiplication. This characteristic is the reason why N can be extracted from the encrypted message during the decryption process. Equations (1) and (2) provide further details for the calculation, as follows:

$$dDS_1 = hE \tag{1}$$

$$dhE = hdE \tag{2}$$

In this example, E is the common starting point for all designs based on this one. Each user's public and private key pair is the single distinguishing factor. Distributing public keys to interested parties is safe because private key information cannot be recovered from a public key. Figure 3 illustrates the procedure by which a user's request for information is handled at the server and demonstrates how safely the content may be accessed. Figure 4 also represents the user and the data that are stored on a cloud server.

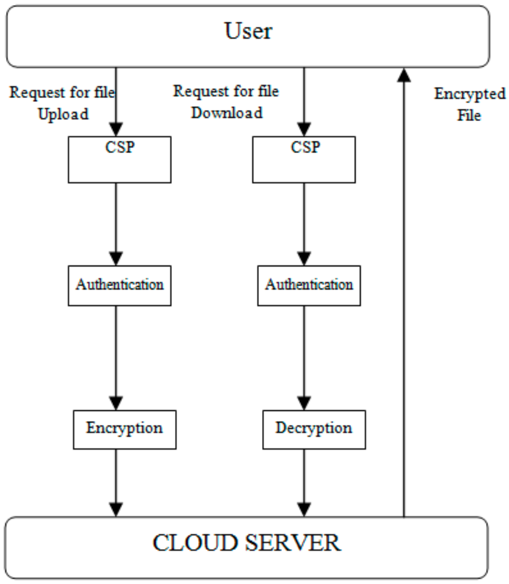

Figure 4. Cloud storage server.

3.2. Blended Suggested Method

The most effective and strong online storage encryption is provided using ECC and AES. The larger key lengths of solo AES makes it slower than the mixture (ECC-AES) approach [11,12] but the shorter key size and faster strong authentication of the blended AES make it faster. Using ECC instead of AES for encryption reduces the size of the key and improves speed. A smaller and more secure key system may be achieved using ECC's usage of industry-standard encryption and decryption keys. In order to protect the data from illegal access, ECC and AES should be used together. Data encryption and decryption will take place after the key size has been determined. ECC generates a key that is utilized with AES to encrypt data. Both ECC and AES work well together to provide a safe system that may be used for cloud storage [13]. Secure data may be stored in less storage space thanks to this technique. Figure 5 shows the suggested algorithm's block diagram.

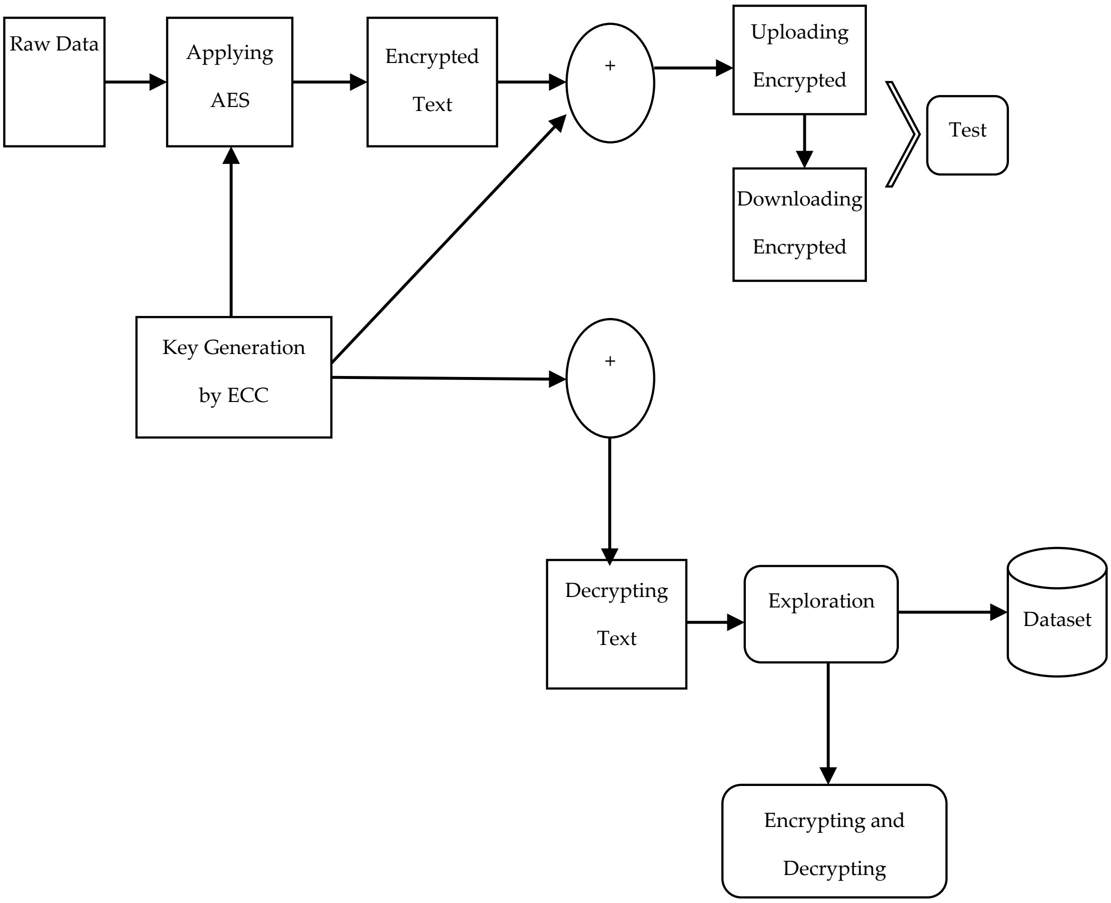

Figure 5. Visualization of ECC and AES algorithm implementation.

It is evident from the preceding section that AES and ECC collaborate to protect cloud-based data. To demonstrate the method's uniqueness, we created a brand new graphic, in which user data are sent securely to the server and are then stored in an encrypted format. It is possible to measure novelty in terms of computing time and cost [14]. For example, if an attacker tries to obtain access to user personal information, or for any other reason, the suggested technique transforms the input file into an encrypted text with the use of AES encryption, such that the encrypted data cannot be deciphered by an unauthenticated user. An assault on the user's file would be pointless since it had already been encrypted before it was sent to the server. If an attack is made against this system, the attacker will be unable to read any data since they will not have the key to decrypt the file.

4. Results and Discussions

By combining ECC and AES, the public storage system is both more secure and more efficient when it comes to encrypting and decrypting data. This indicates that by using these two methods, the user will be able to decipher the original message. ECC is used to protect data stored on the cloud. The use of a smaller key size for data storage may assist in minimizing storage space and in achieving the required outcomes. The RSA employs the same 3072-bit algorithm [15]. A reduced key size and optimized public key encryption are two of the ECC's most helpful features, according to experts. For the reason that photos take longer to encode and decode than textual information, we used three distinct image databases to make a contrast between our suggested approach and the other current methods since pictures typically demand more computation time than textual content. To evaluate performance in a variety of situations, it is necessary to take a variety of picture sizes. Experiments were carried out on 3233, 4830, and 6308 picture datasets. The assessment of encryption time using various techniques is shown in Figure 6. Moreover, the hybrid algorithm is being considered. The hybrid ECC-AES method outpaced the competition in terms of encryption speed thanks to its smaller key size [16]. The advantages of both approaches are combined in the hybrid ECC AES approach, making for a more secure and resilient system. The suggested h method, on the other hand, has a substantially lower encryption time than the existing techniques. Our computing costs decreases as the time it takes to encrypt decreases, which is a great benefit. Due to this, our suggested method is more effective than the existing methods. A comparison of the time taken for decryption using different techniques is shown in Figure 7.

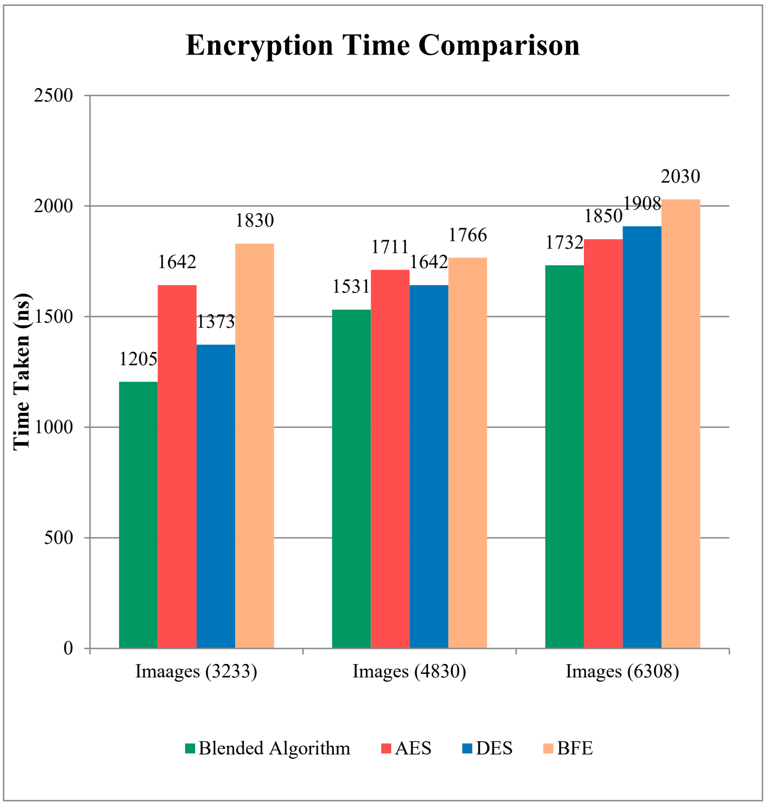

Figure 6. Comparison of the time taken for encryption of data using various techniques.

The algorithm under consideration is a hybrid one. The results show that the decreased key size of the hybrid ECC-AES strategy results in a faster decryption of data than the previous approaches. The hybrid ECC-AES algorithm also includes the special features of both methods, making for a more secure and robust system. The suggested hybrid algorithm's decryption time is much lower than that of the competing techniques, as can also be demonstrated. Decryption takes less time and costs less money; thus, it is a win-win situation. Due to this, our suggested method is more effective than the existing methods.

As a last check, we compared our suggested hybrid algorithm's encryption and decryption times to the existing algorithms (such as AES and DES), as well as to Blowfish (BFE) and DES. A variety of keys, ranging from 64 bits to 256 bits, were used in the experiments. Different keys were used to test the proposed and current encryption techniques for text data. Encryption and decryption times for all the values are presented in seconds in Tables 1 and 2.

Table 1. Encryption duration computed using various key lengths.

Sizes	Combined	Advanced Encryption Standard	Data Encryption Standard	Blowfish Encryption
64	2.52	3.54	4.01	4.43
128	2.59	3.71	4.14	4.59
192	2.66	3.6	4.17	4.55
256	2.72	3.72	4.46	4.82

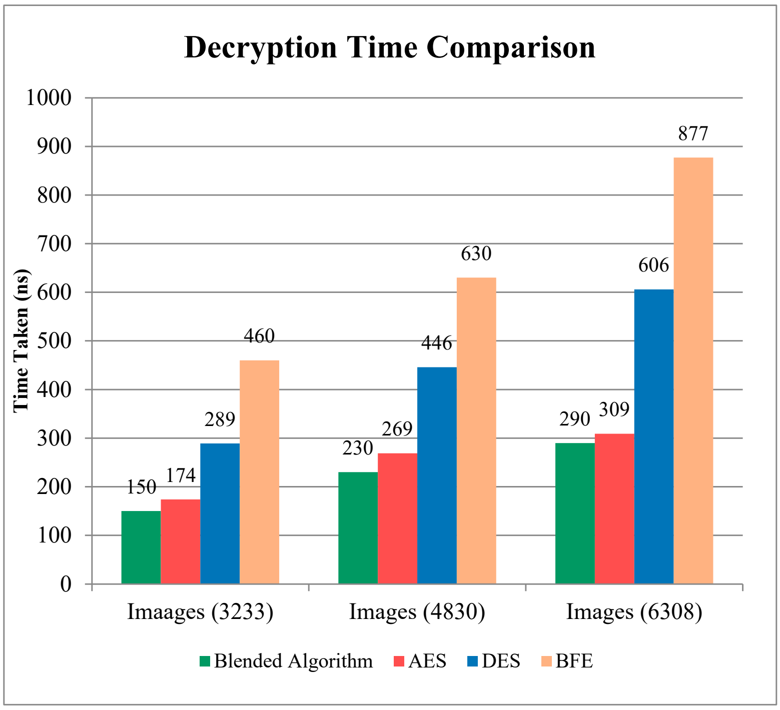

Figure 7. Comparison of the time taken for decryption of data using various techniques.

Table 2. Decryption duration computed using various key lengths.

Sizes	Combined	Advanced Encryption Standard	Data Encryption Standard	Blowfish Encryption
64	1.76	2.81	3.23	4.01
128	1.89	2.94	3.42	4.06
192	2	3.05	3.5	4.22
256	2.22	3.2	3.7	4.37

5. Conclusions and Future Scope

Even if a user has no prior experience with IT, cloud computing and other related services make it possible for everyone to make use of high-quality services. It is possible to access and manage data from any place in the world using a cloud interface supplied by an external party's CSPs through the Internet. The user benefits from a wide range of cloud-based services. The term "user" is used to describe anyone who makes use of a cloud service. Many people would appreciate the option to access their data from any location at a reasonable price. Cloud services may be accessed on any system since there is no need to bring your own device with you. With that said, cloud services have a drawback—poor data security—which may be solved with appropriate tactics and must be guarded. ECC is specifically utilized to lessen the complexity of the procedures during the production of a key. Compared to other cryptographic algorithms, ECC's improvement is much superior to its key size, which is small. A combination of AES and ECC may significantly improve data optimization and security. However, in order to further develop the notion of cloud computing using cryptographic approaches, further security will be required. The hybrid approach's security may be improved in the future to enhance this study. Multiple layers of security could be added to the system to make it more robust and efficient.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data are contained within the article.

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

References

1. Addya, S.K.; Satpathy, A.; Ghosh, B.C.; Chakraborty, S.; Ghosh, S.K.; Das, S.K. CoM CLOUD: Virtual Machine Coalition forMulti-Tier Applications Over Multi-Cloud Environments. *IEEE Trans. Cloud Comput.* **2023**, *11*, 956–970. [CrossRef]
2. Barthwal, V.; Rauthan, M.M.S. AntPu: Ameta- heuristic approach for energy-efficient and SLA aware management of virtual machines in cloud computing. *Memetic Comput.* **2021**, *13*, 91–110. [CrossRef]
3. Cziva, R.; Jouët, S.; Stapleton, D.; Tso, F.P.; Pezaros, D.P. SDN-Based Virtual Machine Management for Cloud Data Centers. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 212–225. [CrossRef]
4. 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]
5. Shen, D.; Luo, J.; Dong, F.; Zhang, J. VirtCo: Joint co flow scheduling and virtual machine placement in cloud data centers. *Tsinghua Sci. Technol.* **2019**, *24*, 630–644. [CrossRef]
6. Hosam, O.; Ahmad, M.H. Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *Int. J. Comput. Sci. Eng.* **2019**, *19*, 153. [CrossRef]
7. 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. Dependable Secur. Comput.* **2019**, *16*, 996–1010. [CrossRef]
8. Jena, O.P.; Tripathy, A.; Swagatam, S.; Rath, S. Dual encryption model for preserving privacy in cloud computing. *Adv. Math. Sci. J.* **2020**, *9*, 6667–6678. [CrossRef]
9. Manaa, M.E.; Hadi, Z.G. Scalable and robust cryptography approach using cloud computing. *J. Discret. Math. Sci. Cryptogr.* **2020**, *23*, 1439–1445. [CrossRef]
10. Henry, N.I.; Anbuananth, C.; Kalarani, S. Hybridmeta-heuristic algorithm for optimal virtual machine placement and migration in cloud computing. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7353. [CrossRef]
11. Niroshini Infantia, H.; Anbuananth, C.; Kalarani, S. Design and Development of Improved Squirrel Search- based Secured VM Migration in the Cloud Sector with Optimal Key Management. *Cybern. Syst.* **2022**, 1–38. [CrossRef]
12. Ray, B.K.; Saha, A.; Khatua, S.; Roy, S. Proactive Fault-Tolerance Technique to Enhance Reliability of Cloud Service in Cloud Federation Environment. *IEEE Trans. Cloud Comput.* **2022**, *10*, 957–971. [CrossRef]

13. Selvam, J.M.; Srivaramangai, P. Time complexity analysis of cloud authentications and data security: Polynomial based hashing and elliptic curve cryptography. *Int. J. Anal. Exp. Modal Anal.* **2020**, *12*, 850–860.
14. Shukla, D.K.; Dwivedi, V.K.; Trivedi, M.C. Encryption algorithm in cloud computing. *Mater. Today Proc.* **2020**, *37*, 1869–1875. [CrossRef]
15. Mirjalili, S. Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. *Knowl.-Based Syst.* **2015**, *89*, 228–249. [CrossRef]
16. Saeed, A.; Garraghan, P.; Hussain, S.A. Cross-VM Network Channel Attacks and Counter measures Within Cloud Computing Environments. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1783–1794. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.