Diyala Journal of Engineering Sciences

Journal homepage: https://djes.info/index.php/djes

ISSN: 1999-8716 (Print); 2616-6909 (Online)

Hybrid Security Model for Medical Image Protection in Cloud

Mohammed Y. Shakor [1*], Nigar M. Shafiq Surameery[2] and Zuheir N Khlaif[3]

[1]Research Centre, University of Garmian, Kalar, Sulaimani, Kurdistan Region, Iraq
[2]Information Technology Department, College of Computer and Information Technology, University of Garmian, Sulaimani, Kurdistan Region, Iraq
[3]Faculty of Educational Sciences, An Najah National University, Nablus, Palestine

ARTICLE INFO

Article history:
Received November 29, 2022
Accepted February 22, 2023

Keywords:
Cloud Storage
Cloud Security
AES
RSA
Healthcare Data

ABSTRACT

A cloud computing environment provides a cost-effective approach for end-users to remotely store and retrieve private data through an internet connection anytime and anywhere. The security of these data cannot always be guaranteed because they can only be accessed by the end-user through a third-party interface, making them vulnerable to potential breaches of authentication and data integrity. This paper presents a secure hybrid approach for a medical image stored in the cloud that prioritises data security and integrity. The suggested model uses a combination of elliptic curve cryptography and advanced encryption standard algorithms to ensure authentication and data integrity. Results demonstrate the superior performance of the proposed model to existing methods, aligning it with compliance requirements for handling sensitive data stored in the cloud. This approach includes adherence to regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), which prescribe specific guidelines for the secure handling, storage and processing of personal information. Contrary to traditional and other hybrid systems, this study suggests that this approach is one of the best in guaranteeing the security of medical images in the cloud.

1. Introduction

Cloud computing is used for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications rather than a direct connection to a server [1].

Cloud technology has become ubiquitous in modern architectures, software design approaches and various services that utilise other technologies [2]. The adoption of cloud computing has led to the development of three main service models: Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) [3,4]. In addition, cloud solutions can be classified into four deployment models: public, private, community and hybrid, depending on the system's requirements. The key benefits of cloud computing include its flexibility, accessibility and capacity when compared with traditional online computing and storage methods [5]. However, cloud computing is also associated with various security concerns [6]. They include privacy and security issues with cloud service providers and security issues that can arise to customers who use these services. Appropriate measures should be implemented to safeguard against potential threats [7] that could involve ensuring the integrity of the cloud provider's infrastructure, implementing data encryption and access controls and performing

* Corresponding author.
E-mail address: mohammed.yousif@garmian.edu.krd
DOI: 10.24237/djes.2023.16107

regular audits and assessments of security protocols [8].

Cloud computing standards provide practical guidelines for utilising computational resources to deliver exceptional performance in various domains, such as computing applications, telecommunication services, social networking and web services [9]. One of the significant advantages of cloud computing is the availability of remote cloud storage, which allows users to access their data from anywhere at any time without any additional burden. However, the primary concern associated with cloud storage is security [10]. Data centres must have robust security mechanisms to ensure the integrity and confidentiality of data stored in the cloud. These mechanisms must be capable of protecting against unauthorised access, data breaches and other potential security threats. Implementing security measures that can verify data storage perfection and data integrity for cloud storage is crucial. Despite the security challenges associated with cloud storage, the benefits of cloud computing are vast, and it remains an attractive option for organisations looking to optimise their IT infrastructure. Nonetheless, implementing stringent security protocols is essential to ensure that the advantages of cloud computing are not offset by the risks that come with it. Consequently, organisations can leverage the full potential of cloud computing while minimising the risks associated with cloud storage [11].

Cryptographic techniques are widely utilised to enhance data security in the cloud. These techniques involve encryption and decryption methods, which rely on distinct keys to protect data from unauthorised access. Two main types of cryptographic techniques are commonly used for data encryption. Firstly, asymmetric key encryption utilises specific public and private keys to encrypt and decrypt data. The public key is used for encryption, whereas the private key is used for decryption, ensuring that the data are secure from unauthorised access. Secondly, symmetric key encryption utilises a single key for data encryption and decryption. This key is maintained secret and must only be shared with authorised parties to allow them to access the encrypted data [12]. By utilising these cryptographic techniques, cloud providers can ensure the confidentiality and integrity of data, challenging the attackers when gaining access to sensitive information [13].

This research proposes a hybrid model of advanced encryption standard (AES) and elliptic curve cryptography (ECC) to ensure the security of data stored on the cloud without involving a third party. The proposed AES–ECC hybrid model is designed to provide efficient protection of the cloud storage system. The key advantage of this hybrid approach is the ability to reduce the key size of the data whilst maintaining the system's security in less time. Several authentication methods for cloud storage are available, but many of them are computationally expensive and time-consuming. The proposed AES–ECC hybrid model offers a relatively efficient alternative that can improve the security of the cloud storage system. The proposed model provides a robust security solution that can protect against various security threats by combining the strengths of AES and ECC. Overall, the proposed hybrid model offers a practical and effective solution for securing data in the cloud without the need for a third party.

The remaining sections of this paper are organised as follows. Section 2 provides the related studies, and Section 3 illustrates the security algorithms' methodology. The proposed hybrid AES–ECC model is presented in Section 4, and Section 5 showcases experimental results and discussions. In Section 6, the conclusion of the work is delivered.

2. Related works

Cloud storage is becoming increasingly popular because all users share resources simultaneously. Data owners prefer it over other providers because cloud storage is always accessible. For this reason, data integrity and preservation should be verified to boost system security.

The researchers in 2021 [14] proposed a method with AES and data encryption standard (DES) algorithms that have been used to maintain user data individually and prevent

conflict with other users to rapidly and easily access their data whilst maintaining a high level of security.

In reference [15], receive side scaling (RSS) and ECC security algorithms were used in 2020 as a hybrid encryption system to protect data in the Software as Service (SaaS) model in the cloud.

An advanced cloud storage privacy paradigm was proposed in [4]. In this study, the blockchain technique and AES are combined to protect data with different data files in the cloud. The result shows a higher level of security more flexibility and less uploading and downloading time and encryption and decryption time than the existing algorithms.

The researchers demonstrated that the encryption of medical images and records and protection of the patient's privacy are legal responsibilities that the existing algorithms may not achieve optimally [16].

For this reason, in 2023, a modified AES algorithm was utilised [17]. The results show that modified AES is more secure than the standard AES for small file sizes. Such systems achieve excellent quality for transitioning from paper health records (PHR) to electronic health records (EHR).

In the study [15], hybrid methods for RSS and ECC are used. When the data have been compressed, some elements that require a signature are provided to the elliptical curve authorities for message digestion and signing. ECC occasionally uses encrypted data for this function. The encryption–decryption procedure is carried out in the same way. Hybrid RSS and ECC analysis algorithms are developed on the basis of their superiority.

Medical image encryption has become mandatory with the enhancement of cloud services and the Internet of Medical Things (IoMT) in 2022 [18]. For this reason, the authors suggested a 3D chaotic map system to protect the medical images and accomplish the best results. After a comparative study with the traditional security systems, the proposed method was trustworthy, offered high robustness and recommended security levels for healthcare utilisation.

Finally, a two-level cryptographic approach and a strategy for enhancing information security in cloud processing were introduced in [19,20]. The model uses the symmetric and uneven encryption calculation (AES and ECC) to enhance information security against intruders, preventing illegal access to natural resources, improving privacy and time required to perform cryptographic tasks and further developing the trust level of the client in the cloud and accelerating the use of more modest keys of ECC in the cryptographic interaction. Table 1 resents the comparative analysis of related works in detail [14-20]

Table 1: Comparative analysis of related works

Refs.	Approach
[14]	Researchers proposed a method that utilises AES and DES algorithms to ensure secure access and storage of individual user data in a cloud environment.
[15]	A hybrid encryption system was used to secure data in the cloud's SaaS model, utilising RSS and ECC security algorithms.
[16]	The study examines various security issues and cutting-edge methods to secure medical images for use with telemedicine systems.
[17]	A modified AES algorithm has been developed and found to be more secure than the standard AES algorithm for small files.
[18]	The authors proposed a 3D chaotic map system to protect medical images and achieve optimal results. The proposed method was reliable, offering high robustness and recommended security levels suitable for use in healthcare.
[19]	A new modulo function-based lightweight digital signature algorithm is proposed to ensure data integrity. This security framework provides high data security, accessibility and integrity for the user data.
[20]	Proposed data security in cloud computing using AES under Heroku cloud. The performance evaluation shows that AES cryptography is robust.

3. Security algorithm methodology

3.1 Advanced Encryption Standard

AES is a symmetric key encryption algorithm that uses a fixed block size of 128 bits and key sizes of 128, 192 or 256 bits [21]. The algorithm works by repeatedly applying a set of mathematical operations, known as rounds, to the input data (the plaintext) and the encryption key. The number of rounds used in the encryption process depends on the key size [22].

The AES algorithm possesses several key features that make it crucial for encrypting medical images in cloud storage.

1. *Confidentiality:* AES encryption provides a high level of confidentiality by converting the original image into a ciphertext that is unreadable without the decryption key. In this approach, only authorised parties can view the medical images [23].
2. *Integrity:* AES uses a key and a block cypher to encrypt data, thereby providing integrity protection. Thus, medical images are not tampered with or modified during transmission or storage [24].
3. *Authentication:* AES encryption can be combined with authentication methods, such as digital signatures to ensure that medical images are obtained from a trusted source [25].
4. *Scalability:* AES encryption is highly scalable, making it well-suited for cloud storage. It can encrypt large amounts of data rapidly and efficiently, making it suitable for storing large medical image files [26].
5. *Compatibility:* AES is a widely accepted and standardised encryption method that can be integrated with various cloud storage providers and platforms [27].
6. Performance: AES is a fast encryption algorithm well-suited for real-time applications. It can encrypt and decrypt large amounts of data rapidly, making it suitable for storing and transmitting medical images [28].

AES is a widely used and accepted standard for symmetric key encryption and is considered very secure. It is used in various applications, including online transactions, secure communications and data storage. However, AES encryption is vulnerable to certain types of attacks, such as side-channel attacks. It should also be used in conjunction with other security measures to provide complete security.

AES-256 is a specific variant of the AES encryption algorithm that uses a 256-bit key. The encryption process of AES-256 is similar to that of other AES variants but with a few key differences.

The following are the main steps for the AES encryption algorithm [29,30]:

1. The plaintext state (128-bit block) is initialised as a matrix of bytes.
2. AddRoundKey: XOR is the initial state with the first-round key derived from the encryption key.
3. Fourteen rounds are performed, each consisting of the following operations:
   - SubBytes: each byte of the state is replaced with a corresponding value from a fixed substitution table (S-box).
   - ShiftRows: the rows of the state matrix are shifted by a fixed number of positions.
   - MixColumns: the columns of the state matrix are mixed by applying a fixed linear transformation.
   - AddRoundKey: XOR is the state with the round key derived from the encryption key.
4. The final round is performed, similar to the previous rounds, but without the MixColumns operation.
5. The final state of the matrix is the ciphertext.

The key schedule for AES-256 is more complex than the other AES variants because it needs to generate 15 round keys from the 256-bit key. AES-256 is considered to be even more secure than AES-128 or AES-192 because of its larger key size. However, it is also slower and more resource-intensive to implement. The use of AES-256 and other security measures is essential to provide complete security.

AES-256 can effectively secure medical images. It provides a high level of security, causing difficulty for an attacker to decrypt the data without the accurate key. Medical images are often sensitive, and personal information should be protected from unauthorised access; AES-256 can encrypt the images prior to transmission or storage [31].

In addition, AES-256 encryption can be used to ensure compliance with regulations, such as Health Insurance Portability and Accountability Act (HIPAA), which requires that medical images be secured to protect patient privacy [32].

However, encryption is only one aspect of securing medical images, and other security measures, such as access control, secure storage and regular backups, should also be implemented.

3.2 Elliptic Curve Cryptography

ECC is a public-key cryptography based on the mathematics of elliptic curves [33]. It is a relatively new technique that is becoming increasingly popular because of its ability to provide the same level of security as Rivest–Shamir–Adleman (RSA), a widely used public-key algorithm with much smaller key sizes. Thus, ECC becomes more efficient and less prone to attack.

A general overview of the ECC cryptographic algorithm [34] is as follows:

1. A specific elliptic curve (e.g., National Institute of Standards and Technology (NIST) P-256) is selected.
2. A private key, typically a random number, which will be used to derive the public key, is generated.
3. The corresponding public key is derived by performing a mathematical operation on the private key and a fixed point (generator) on the curve.
4. The sender uses the recipient's public key to encrypt the message.
5. The recipient uses the private key to decrypt the message.
6. The sender uses their private key to generate a signature for the message.
7. The recipient uses the sender's public key to verify the signature.

ECC is considered more secure than RSA because factorising large integers, the basis of RSA security, is more challenging [35][36]. ECC is also more efficient and requires smaller key sizes to provide the same level of protection. As a result, ECC becomes particularly well-suited for use in applications, such as cloud services and the Internet of Things (IoT), where computational resources are limited [37].

4. Hybrid proposed model

AES–ECC hybrid model can be considered an advanced, effective and popular encryption technique to secure sensitive images in cloud storage. AES is a symmetric key encryption algorithm widely used for encrypting data. It uses the same key for encryption and decryption, making it fast and efficient. Hybrid algorithms ensure that the images are protected from unauthorised access during storage and transmission by encrypting the medical images using AES. On the contrary, ECC is an asymmetric key encryption algorithm that uses a pair of keys: a public key for encryption and a private key for decryption. ECC is known for its security and efficiency for key sizes much smaller and faster than RSA and DSA, which are popular algorithms for key generation. Moreover, whilst RSA is a popular algorithm for key generation, ECC is better suited for generating AES keys for image encryption and decryption in cloud storage given its superior security, efficiency, key exchange capabilities and scalability. ECC's smaller key size makes it more secure than RSA whilst also requiring fewer computational resources for faster processing of large image files.

By generating the AES key with 256 bits using ECC, the hybrid algorithms ensure that only authorised users, who hold the corresponding ECC private key, can decrypt the images, preventing unauthorised access to the images, even if an attacker could access the encrypted images in the cloud.

The pseudocode for the hybrid AES–ECC model is shown in the following section.

Step 1: An elliptic curve key pair (private key and public key) is generated.

private key = ECC.generate_private_key ()

public key = ECC.generate_public_key(private_key)
Encryption process
Step 2: A shared secret using the recipient's public key is produced.
shared_secret = ECC.generate_shared_secret(recipient_public _key, private_key)
Step 3: The shared secret is used to generate an AES key.
aes_key = AES.generate_key(shared_secret)
Step 4: The AES key is used to encrypt the image.
encrypted_image = AES.encrypt(image, aes_key)
Step 5: The encrypted image is stored in cloud storage.
cloud_storage.store(encrypted_image)
Decryption process
Step 6: The encrypted image is retrieved from cloud storage
encrypted_image = cloud_storage.retrieve()
Step 7: The shared secret is used to regenerate the AES key.
aes_key = AES.generate_key(shared_secret)
Step 8: The AES key is used to decrypt the image.
decrypted_image =AES.decrypt(encrypted_image, aes_ke y)

The contribution of this work, as shown in Figure 1, includes the development of a secure and efficient medical image encryption and decryption model by combining the strengths of AES and ECC encryption algorithms. This hybrid model is designed to prevent unauthorised access to sensitive images in the cloud by using a shared secret generated by ECC. Furthermore, an AES key that encrypts the image is generated using ECC. The use of ECC provides an additional layer of security given that the image can only be decrypted by authorised users, who hold the corresponding ECC private key. As a result, unauthorised access to sensitive images is prevented, even if an attacker gains access to the encrypted images in the cloud. The proposed hybrid AES–ECC model can be applied in various applications that require secure image encryption and decryption, such as medical imaging, military and defence and financial institutions.

The hybrid model was used to test Medical Segmentation Decathlon dataset images with different resolutions. This model has been tested in a Python environment and hosted on Hostinger, a highly available, scalable, cost-effective and user-friendly cloud hosting platform with the following specifications: RAM: 3 GB, SSD Storage: 200 GB, CPU Cores: 2 Cores, Bandwidth: Unlimited, I/O (KB/s): 10240.

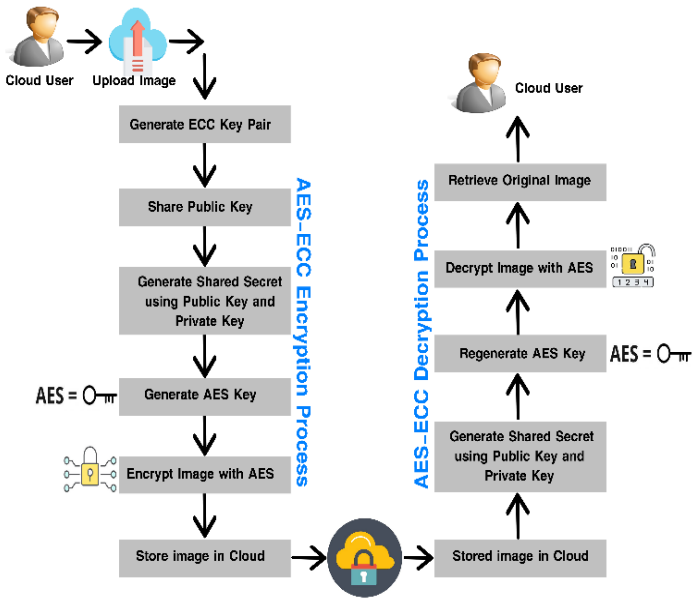

Figure 1. AES–ECC encryption and decryption diagram

5. Results and discussion

This section compares the hybrid AES–ECC model system with traditional AES and other hybrid systems.

This study aims to determine each technique's encryption and decryption speeds under consideration for various image sizes. The throughput and the average encryption and decryption times for the hybrid AES–ECC model and the traditional AES and AES–RSA model were measured.

$$\text{Throughput} = \frac{\text{Plaintext (KB)}}{\text{Encryption time (Sec.)}}. \quad (1)$$

AES–ECC implemented faster encryption and decryption in the cloud storage, as shown in Tables 2 and 3. The standard AES required 27623, 30034 and 35998 ms to encrypt the three different file sizes (559, 636 and 910 kb), which were selected randomly from the dataset in Section 4 and tested in the experiment. Comparatively, the Hybrid AES–ECC model's encryption times for the same file sizes were 23335, 26231 and 32997 ms. In addition, the standard AES decryption required 28901, 30921 and 41830 ms for the various file sizes. On the contrary, the Hybrid AES–ECC model required 24735, 27132 and 34692 ms to decrypt the selected image file.

Table 2: AES–ECC and Traditional AES Encryption Time

File Size (kb)	Encryption Time in (ms)	
	Hybrid Model AES-ECC	**Traditional AES**
559	23335	27623
636	26231	30034
910	32997	35998
Total time	82563	93655
Throughput	0.025495682	0.022476109

Table 3: AES–ECC and Traditional AES Decryption Time

File Size (kb)	Decryption Time in (ms)	
	Hybrid Model AES-ECC	**Traditional AES**
559	24735	28901
636	27132	30921
910	34692	41830
Total time	86559	101652
Throughput	0.024318673	0.020707905

The results obtained from the experiments reveal that the proposed hybrid model algorithm offers significantly better performance than the traditional AES algorithm in terms of encoding and decoding time for medical images of varying sizes. Tables 2 and 3 provide detailed insights into the encoding and decoding time for different file sizes. The results evidently show that the proposed hybrid model significantly improves the encoding and decoding time compared with the traditional AES algorithm.

Specifically, the proposed hybrid model algorithm displays an average encoding time of 3697.33 ms, which is lower than the traditional AES algorithm. Similarly, the proposed algorithm demonstrates an average decoding time of 5031 ms, which is also lower than the traditional AES algorithm. These results highlight the efficiency and effectiveness of the proposed hybrid model algorithm in securing medical images with minimal processing time.

The present study has also compared the proposed AES–ECC model and another hybrid model, AES–RSA. The findings revealed that the AES–ECC model outperformed the AES–RSA model in terms of computational efficiency and encryption and decryption times. Specifically, the AES–ECC model recorded an average time used in encoding all file sizes that was considerably lower than that of the AES–RSA model, as evidenced by the results presented in Table 4. Similarly, Table 5 demonstrates that the average time used in decoding all file sizes was significantly lower for the AES–ECC model than the AES–RSA model.

Moreover, the comparison revealed that the AES–ECC model used smaller key sizes than AES–RSA to achieve the same level of security, indicating the superiority of ECC over RSA in terms of security. The results also showed that the AES–ECC model was more suitable for cloud storage because of its scalability in handling large amounts of data. Overall, the present findings suggest that the proposed AES–ECC model can provide improved security, efficiency and speed for the encryption and decryption of medical images in cloud storage compared with the AES–RSA hybrid model.

Table 4: AES–ECC and AES–RSA Encryption Time

File Size (kb)	Encryption Time in (ms)	
	AES–RSA	AES–ECC
559	25782	23335
636	28250	26231
910	34854	32997
Total time	88886	82563
Throughput	0.02368202	0.025495682

Table 5: AES–ECC and AES–RSA Decryption Time

File Size (kb)	Decryption Time in (ms)	
	AES–RSA	AES–ECC
559	27425	24735
636	29980	27132
910	38177	34692
Total time	95582	86559
Throughput	0.022022975	0.024318673

Considering the data in Tables 2–5, the throughput for hybrid AES–ECC for the selected image sizes is 0.025495682 and 0.024318673, whereas 0.022476109 and 0.020707905 are recorded for standard AES. However, AES–RSA throughputs were 0.02368202 and 0.022022975.

The results indicate that the hybrid AES–ECC has a greater throughput than others. The present study has been subjected to comparison with the previously conducted studies [38] and [39]. The outcome of the comparative analysis revealed that this study exhibited superior performance to the existing investigations.

6. Conclusions

IT-related services, such as cloud computing, provide efficient services regardless of the user's knowledge about technology. Cloud services offered by third-party providers via the internet allow for easy storage, management, improvement and data access via a cloud interface, regardless of user location. The drawback of cloud services in sensitive states is the low data security, which may be overcome through special strategies. An improved image encryption scheme based on MAE–ECC as the hybrid system is suggested because protecting medical image information is a legal requirement. AES resolves the difficult calculation issue, and ECC is used for symmetric key sharing. In summary, the results of hosting the proposed AES–ECC system demonstrated its superior performance to the standard AES and another hybrid system in terms of encryption and decryption time . Finally, the proposed algorithm can offer a highly efficient and effective solution for encrypting large medical images with enhanced security measures, which could have significant implications for medical data storage and sharing in the cloud.

References

[1] Z. Zhu, A. X. Liu, and F. Chen, 'FPGA Resource Pooling in Cloud Computing', IEEE Trans. Cloud Comput., vol. PP, no. c, p. 1, 2018, doi: 10.1109/TCC.2018.2874011.

[2] I. A. Elgendy, W. Zhang, C. Liu, and C. Hsu, 'An Efficient and Secured Framework for Mobile Cloud Computing', vol. 7161, no. c, pp. 1–10, 2018, doi: 10.1109/TCC.2018.2847347.

[3] J. Wang, J. Pan, F. Esposito, P. Calyam, Z. Yang, and P. Mohapatra, "Edge Cloud Offloading Algorithms," ACM Computing Surveys, vol. 52, no. 1, pp. 1–23, Feb. 2019, doi: 10.1145/3284387.

[4] M. Shakor, M. Khaleel, and F. Abed, "Enhancing Cloud Storage Privacy (CSP) Based on Hybrid Cryptographic Techniques," Journal of Garmian University, vol. 6, no. 1, pp. 582–594, Apr. 2019, doi: 10.24271/garmian.2000.

[5] S. Raghavendra et al., "Critical Retrospection of Security Implication in Cloud Computing and Its Forensic Applications," Security and Communication Networks, vol. 2022, pp. 1–19, May 2022, doi: 10.1155/2022/1791491.

[6] C. Liu, Z. Su, X. Xu, and Y. Lu, 'Robotics and Computer-Integrated Manufacturing Service-oriented industrial internet of things gateway for cloud manufacturing', Robot. Comput. Integr. Manuf., vol. 73, no. July 2021, p. 102217, 2022, doi: 10.1016/j.rcim.2021.102217.

[7] B. Alaya and L. Sellami, 'Journal of Information Security and Applications Clustering method and symmetric / asymmetric cryptography scheme adapted to securing urban VANET networks', J. Inf. Secur. Appl., vol. 58, p. 102779, 2021, doi: 10.1016/j.jisa.2021.102779.

[8] T. Wang, Y. Zhou, H. Ma, and R. Zhang, "Enhanced Dual-Policy Attribute-Based Encryption for Secure Data Sharing in the Cloud," Security and Communication Networks, vol. 2022, pp. 1–21, May 2022, doi: 10.1155/2022/1867584.

[9] T.-Y. Youn and H. S. Rhee, "Secure Symmetric Keyword Search with Keyword Privacy for Cloud Storage Services," Security and Communication

Networks, vol. 2021, pp. 1–8, Nov. 2021, doi: 10.1155/2021/2291470.

[10] F. Alidadi, S. Shaghayegh, and B. Chehelcheshmeh, 'A cloud - based mobile payment system using identity - based signature providing key revocation', J. Supercomput., no. 0123456789, 2021, doi: 10.1007/s11227-021-03830-4.

[11] D. He and S. Xiong, "Image Processing Design and Algorithm Research Based on Cloud Computing," Journal of Sensors, vol. 2021, pp. 1–10, Oct. 2021, doi: 10.1155/2021/9198884.

[12] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," Multimedia Tools and Applications, vol. 80, no. 14, pp. 21165–21202, Mar. 2021, doi: 10.1007/s11042-021-10723-4.

[13] S. Domanal, S. Member, R. Mohana, R. Guddeti, and S. Member, 'A Hybrid Bio-Inspired Algorithm for Scheduling and Resource Management in Cloud Environment', vol. X, no. X, pp. 1–14, 2017, doi: 10.1109/TSC.2017.2679738.

[14] H. S. Yahia et al., 'Comprehensive Survey for Cloud Computing Based Nature-Inspired Algorithms Optimization Scheduling', vol. 8, no. 2, pp. 1–16, 2021, doi: 10.9734/AJRCOS/2021/v8i230195.

[15] H. Li, C. Lan, X. Fu, C. Wang, F. Li, and H. Guo, "A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing," Sensors, vol. 20, no. 17, p. 4720, Aug. 2020, doi: 10.3390/s20174720.

[16] A. Odeh and Q. A. Al-haija, 'Medical image encryption techniques : a technical survey and potential challenges', no. January, pp. 3170–3177, 2023, doi: 10.11591/ijece.v13i3.pp3170-3177.

[17] N. M. S. Surameery, 'Modified Advanced Encryption Standard for Boost Image Encryption', vol. 6, no. 1, pp. 1–4, 2022, doi: 10.21928/uhdjst.v6n1y2022.pp52-59.

[18] J. Srivastava, S. Routray, S. Ahmad, and M. M. Waris, "Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–17, Jul. 2022, doi: 10.1155/2022/7218113.

[19] B. Prabhu Kavin, S. Ganapathy, U. Kanimozhi, and A. Kannan, "An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA," Wireless Personal Communications, vol. 115, no. 2, pp. 1107–1135, Jun. 2020, doi: 10.1007/s11277-020-07613-7.

[20] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), Apr. 2018, doi: 10.1109/wocc.2018.8372705.

[21] S. Roldán, L. Fatih, and B. Subhadeep, 'Six shades lighter : a bit-serial implementation of the AES family', J. Cryptogr. Eng., vol. 11, no. 4, pp. 417–439, 2021, doi: 10.1007/s13389-021-00265-8.

[22] C. Jacobs et al., "Finding high-redshift strong lenses in DES using convolutional neural networks," Monthly Notices of the Royal Astronomical Society, vol. 484, no. 4, pp. 5330–5349, Jan. 2019, doi: 10.1093/mnras/stz272.

[23] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," The Journal of Supercomputing, vol. 75, no. 10, pp. 6663–6682, May 2019, doi: 10.1007/s11227-019-02878-7.

[24] A. K. Et. al., "An Information Security Using DNA Cryptography along with AES Algorithm," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 1S, pp. 183–192, Apr. 2021, doi: 10.17762/turcomat.v12i1s.1607.

[25] N. Kheshaifaty and A. Gutub, "Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication," Journal of Engineering Research, Nov. 2021, doi: 10.36909/jer.13761.

[26] H. E. Hassan, M. Tahoun, and G. S. Eltaweel, 'ORIGINAL ARTICLE A robust computational DRM framework for protecting multimedia contents using AES and ECC', Alexandria Eng. J., 2020, doi: 10.1016/j.aej.2020.02.020.

[27] Y. Naito, Y. Sasaki, and T. Sugawara, 'AES-LBBB : AES Mode for Lightweight and BBB-Secure Authenticated Encryption', IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2021, no. 3, pp. 298–333, 2021, doi: 10.46586/tches.v2021.i3.298-333.

[28] H. M. Mohammad and A. A. Abdullah, 'Enhancement process of AES : a lightweight cryptography algorithm-AES for constrained devices', vol. 20, no. 3, pp. 551–560, 2022, doi: 10.12928/TELKOMNIKA.v20i3.23297.

[29] M. Nabil, A. A. M. Khalaf, and S. M. Hassan, 'Design and implementation of pipelined and parallel AES encryption systems using FPGA', vol. 20, no. 1, pp. 287–299, 2020, doi: 10.11591/ijeecs.v20.i1.pp287-299.

[30] F. T. Abdul Hussien, A. M. S. Rahma, and H. B. Abdul Wahab, "A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites," Security and

Communication Networks, vol. 2021, pp. 1–15, Dec. 2021, doi: 10.1155/2021/9961172.

[31] B. Jacobs and J. Popma, 'Medical research , Big Data and the need for privacy by design', no. June, pp. 1–5, 2019, doi: 10.1177/2053951718824352.

[32] J. Gutiérrez-martínez, M. A. Núñez-gaona, and H. Aguirre-meneses, 'Business Model for the Security of a Large-Scale PACS , Compliance with ISO / 27002 : 2013 Standard', pp. 481–491, 2015, doi: 10.1007/s10278-014-9746-4.

[33] B. R. B. P. Chitra, 'ECC - CRT : An Elliptical Curve Cryptographic Encryption and Chinese Remainder Theorem based Deduplication in Cloud', Wirel. Pers. Commun., no. 0123456789, 2020, doi: 10.1007/s11277-020-07756-7.

[34] S. Banerjee and A. Patil, "ECC Based Encryption Algorithm for Lightweight Cryptography," Intelligent Systems Design and Applications, pp. 600–609, Apr. 2019, doi: 10.1007/978-3-030-16657-1_56.

[35] L. Ertaul and W. Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)," Lecture Notes in Computer Science, pp. 102–113, 2005, doi: 10.1007/11422778_9.

[36] N. M. S. Surameery and M. Y. Shakor, "CBES: Cloud Based Learning management System for Educational Institutions," 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Surabaya, Indonesia, 2021, pp. 270-275, doi: 10.1109/EIConCIT50028.2021.9431932.

[37] N. M. S. Surameery and M. Y. Shakor, "Blockchain as a foundation to support healthcare systems". International Journal of Nonlinear Analysis and Applications. 2022 Dec 5, doi: https://doi.org/10.22075/ijnaa.2022.7186.

[38] R. Lin and S. Li, "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm," Security and Communication Networks, vol. 2021, pp. 1–18, Apr. 2021, doi: 10.1155/2021/5586959.

[39] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," IEEC 2022, Jul. 2022, doi: 10.3390/engproc2022020014.