Secure Cloud Authentification Using AES Encryption

Leila Megouache[1,*], Salheddine Sadouni[1], Ouissal Sadouni[2], Mahieddine Djoudi [3] and Abdelhafid Zitouni[4]

[1]*Department of Geographical Sciences and Topography, Freres Mentouri Constantine 1 Univeristy, Department of Geographical Sciences and Topography. Constantine, Algeria*

[2]*University of Constantine3- Algeria, 25000 Constantine, Algeria*

[3]*TECHNE Labs, University of Poitiers, 1 rue Raymond Cantel, 86073 POITIERS CEDEX 9, France.*

[4]*LIRE Laboratory, Computer Science Department, University of Constantine 2- Algeria, 25000*

Abstract

Nowadays, the Cloud has become an essential technology and the data stored there is generally of a sensitive nature and this is the reason why malicious people want to corrupt the data hosted. Given the number of attacks which overwhelm the latter every second, security components such as firewalls or existing intrusion detection systems are not suitable for detecting distributed attacks which are subdivided into sub-attacks in order to be undetectable. By such a security system. It should be mentioned that if authenticated access is not clearly identified, then it will be impossible to trace the connection and the resulting modification of the data or service. For this we will propose a data encryption solution which will use the techniques of AES to secure cloud authentication and ensuring the integrity of the data. This solution will ensure data preservation and security in a more reliable manner.

Keywords

Data Security, Cloud Computing, Authentication, Encryption, Privacy, Risks and threats

1. Introduction

Cloud computing plays an essential role in the architecture of the new generation of IT systems within companies [1]. On the other hand, management and security in the Cloud have remained similar to those employed in traditional IT systems [2]. Unlike traditional solutions, Cloud Computing transfers software and data to external data centers located on providers' premises, making it difficult to manage and control data and services with reliability and confidence [3]. However, these traits pose many new security challenges.

Cloud computing security refers to the measures and practices put in place to protect data, applications and infrastructure hosted in cloud computing environments [4]. It aims to guarantee the confidentiality, integrity, availability and compliance of information stored and processed in the Cloud. This involves the use of various technologies, policies and procedures to prevent threats such as cyberattacks, data leaks, privacy breaches and service interruptions [5]. In summary, cloud computing security aims to create a reliable and secure environment for users and organizations that use cloud services to store, manage and access their data and applications.

In 2009, a survey conducted by the International Data Corporation IDC revealed that 74% of IT managers and business people considered security concerns related to cloud computing to be the main barrier preventing them from using cloud services [6]. However, there is still a need to adequately address privacy, security, reliability, and interoperability issues; in particular, data security and privacy issues are of great importance and priority. Thus, it is essential that the research field takes these

Tunisian-Algerian Conference on applied Computing (TACC 2024), Constantine, Algeria

*Corresponding author.

†These authors contributed equally.

0009-0002-6753-8174 (L. Megouache); 0000-0002-1673-4610 (O. Sadouni); 0000-0002-2998-55747 (M. D.); 0000-0003-2498-4967 (A. Zitouni)

concerns into consideration by offering and establishing strong protection mechanisms in order to exploit the benefits of Cloud Computing without compromising security and confidentiality [7]. We take the example of the article [8] to ensure the authentication of user access to their data and applications, the authors proposed AuthFlow, an authentication and access control mechanism based on user credentials. The user. 'Host. Their main contributions were a host authentication mechanism just above the MAC layer in an OpenFlow network, which ensures low overhead and provides fine-grained access control; and credential-based authentication to perform access control based on the privilege level of each host, by mapping the host's credentials to the set of flows that belong to the host.

To minimize these problems, we propose a new remote access control system that guarantees secure communication and authentication between cloud multi-users and their data. The data is different in nature, therefore, whenever a user changes their location, they need to register with the nearest trusted authority. We offer remote user registration via the access control mechanism which takes place in two phases, the remote authentication phase and the key agreement phase, during which, after successful authentication, a session key will be calculated using techniques AES cryptographic files. The calculated session key will be used to ensure secure communications in the future. The AES standard (Advanced Encryption Standard) is used in this approach, data encrypted using AES before being uploaded to a cloud. The SMS (Short Message Service) alert mechanism will be taken into account to prevent unauthorized access to user data. A security analysis and security verification will be applied to show the reliability of our system by comparing it with other existing systems in terms of calculation costs.

This paper is presented as follows. The related works are discussed in Section 2. The proposed solution is explained in Section 3. The discussions and result in Section 4. Finally, the conclusion are given in Section 5.

2. Related Work

In this part, we analyze a variety of security solutions. Several improved authentication protocols have been proposed telling us that:

The virtual access techniques in [9] are used to ensure the confidentiality of user profiles and the protection of their data, making it possible to apply security protocols to the different layers of the Cloud. Confidentiality can be achieved by using appropriate encryption techniques taking into account the encryption type. In reality, it all depends on the security policy of the Cloud provider and also depends on whether customers decide to encrypt their data before downloading it, taking into account the encryption type.

In [10], authors examined access control solutions used by organizations as a cyber security strategy for authorizing users and data to access cloud computing, the Internet of Things (IoT), blockchain, and networks defined by software (SDN).

In their article [11], authors studied the trends in blockchain technology with IoT. Additionally, the paper highlights blockchain-based IoT applications to bring more security to IoTs.

The article [12] has proved the need for intra- and inter-cloud authentications to protect cloud service providers against threats. for this, one of the open source cloud software, called Reddit, was audited.

In [13], authors offer a three-factor authentication protocol based on ECC which guarantees the confidentiality of patients affected by covid 19, they offer secure access based on mutual authentication. Session key security has been carried out using BAN logic and the ROR model.

In [14], to ensure security, confidentiality and authentication of data between the patient and the healthcare service provider, authors proposed a system that will focus on the development of an IoT-based CHD system to improve authentication and data security in a cloud environment.

Awan et al. [15] proposed a 128 AES method to speed up the encryption process. The technique uses less energy, better load balancing and improved trust and resource management on the network.

In [16] Shah and Philip mentioned that authentication plays a vital role in data security. The biometrics system was used for authentication to create a biometric cloud for online signature recognition making the signature recognition system more scalable and faster. This system, based on biometrics, can be used successfully in banking and e-commerce applications.

Finally, one of the most effective and cost-effective solutions to ensure data security and authentication is the implementation of cloud computing technologies [17-18]

3. Proposed Solution

Our proposal work is based on the principle of encryption to ensure and guarantee the security of data hosted in the Cloud, nevertheless, there are several data encryption algorithms and each one has these advantages and disadvantages, in the solution we are going to present, The user can have complete confidence that, this data can be stored securely in a Cloud provider without fear of loss or risk of hacking. In our work, we used encryption with the AES algorithm [19], and which allows access and downloading of data while ensuring the integrity of this data thanks to a MAC protocol. The proposed solution depends on three basic elements or rather three key words, namely data encryption, AES algorithm and data integrity, these are the three factors we focus on in our work.

3.1. Data encryption

For data encryption, we have chosen to work with symmetric encryption [15]. Secret key (symmetric) algorithms are algorithms, where the encryption key can be calculated from the decryption key or vice versa. In our case, the encryption key and the decryption key are the same. Here is a diagram which illustrates the principle of secret key encryption.

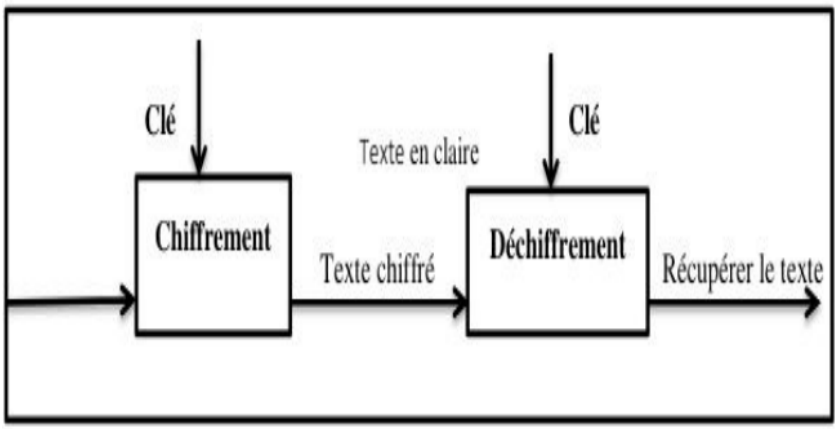

Figure 1: Symmetric cryptography

The AES algorithm which is a symmetric block encryption method [16], In summary, AES is widely adopted due to its proven security, high performance and versatility, making it a popular choice for ensuring privacy data in many applications and environments. AES includes several encryption modes [20], and for our work, we used the CBC blockchain mode which is illustrated in Figure 2.

Different key sizes do not mention how the algorithm works. The only difference is in the number of times the four operations of the second phase are performed. Figure 3 indicates the number of iterations (Nr) carried out. This number depends on the number of columns contained in the matrix containing the key (Nk), as well as, its number of rows (Nb). So, in 128-bit AES, the number of loop turns will be equal to Nr - 1. Its operation takes place in several stages (usually called "rounds").

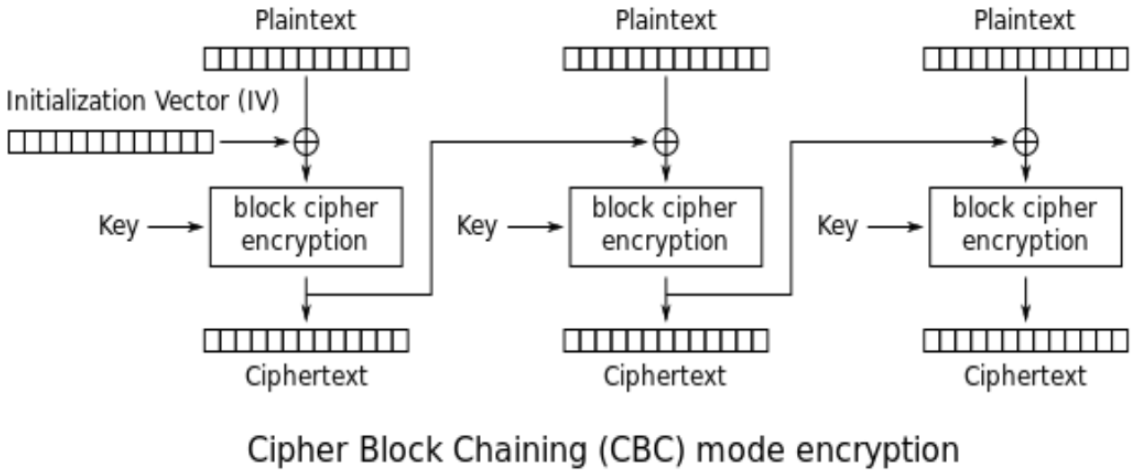

Figure 2: Encryption mode

	Nk	Nb	Nr
128	4	4	10
192	6	4	12
256	8	4	14

Figure 3: Number of iterations with respect to the key.

The initial round allows to perform an initial key operation. Then, four operations are repeated nine times. These operations are:

- **SubBytes**
  This operation [21] allows to make a non-linear substitution on the state 8 matrix. Each byte is replaced by another byte chosen from another table, called SBox. This S-Box is a two-dimensional array with 16 boxes in X and Y, which represents 256 distinct values. Let's take the example of the letter A which has the ASCII value 65 or 0100 0001 in binary. By separating these 8 bits into two groups of 4 bits, the values are 4 and 1. These two values correspond to the x and y indices of the matrix which point to the new value of A.

- **Shift Rows**
  In this step, each box of the table modified by the previous step is shifted [22]. If we represent the data of the state matrix in the form of a matrix of 4 boxes by 4 (each box containing 8 bits which always makes a total of 128 bits), the first line is shifted by 0 positions to the left, the second line is shifted by one position, the third line by two positions and the fourth line by three positions as indicated in Figure 4 below.

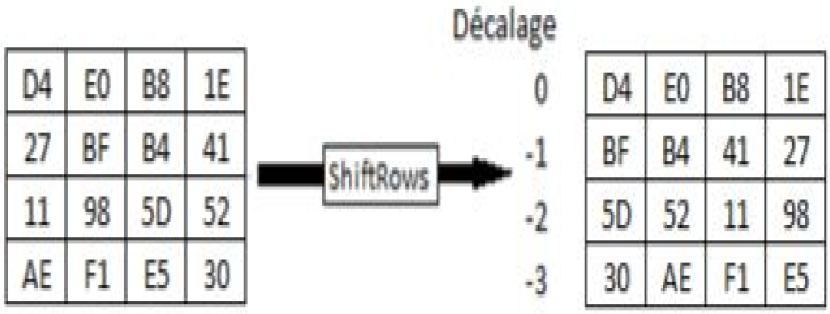

Figure 4: ShiftRows Operation

- **MixColumns**
  In this step, we calculate the matrix product between each column of the state matrix and another matrix [23]. Mathematically, this other matrix is calculated with finite fields of 28 elements. For instance, the state column used is a polynomial a(x) of degree 3. The polynomial

$$c(x) = 03x3 + x2 + x + 02. \tag{1}$$

  Then, to calculate the new values, the following calculation is carried out:

$$a(x) * c(x) mod(x4 + 1). \tag{2}$$

  It is important to emphasize that the modulo achieved here is not obvious. It allows you to always come across a number between 0 and 255. Then, c(x) and (x4 + 1) must be co prime, otherwise the result of the modulo could give 0. If this is the case, the data would not be deciphered by performing the reverse operation.
  Computationally, these calculations are performed as matrix products [24]. Taking the example in Figure 5, the calculation would look as follows to obtain the first value of the column:

$$2 * D4 + 3 * BF + 1 * 5D + 1 * 30. \tag{3}$$

  Then the same calculation is applied to the second row of the matrix, and so on, giving the new values.

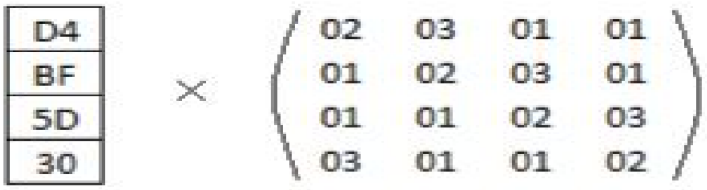

Figure 5: MixColum Operation

- **KeyExpansion**
  Before proceeding to the next step “AddRoundKey”, the key needs to be changed [25]. The first column of the key once modified will correspond to the last column, shifted from bottom to top. Then, it will be modified with the SBox [26], then an xor operation will be carried out between the result obtained, the first column of the original key and the column x (x corresponds to the round number) of the Rcon matrix (fixed table of revolution constants). The other three remaining columns will then be Xor operations between the original key column and the last column added to the new key.

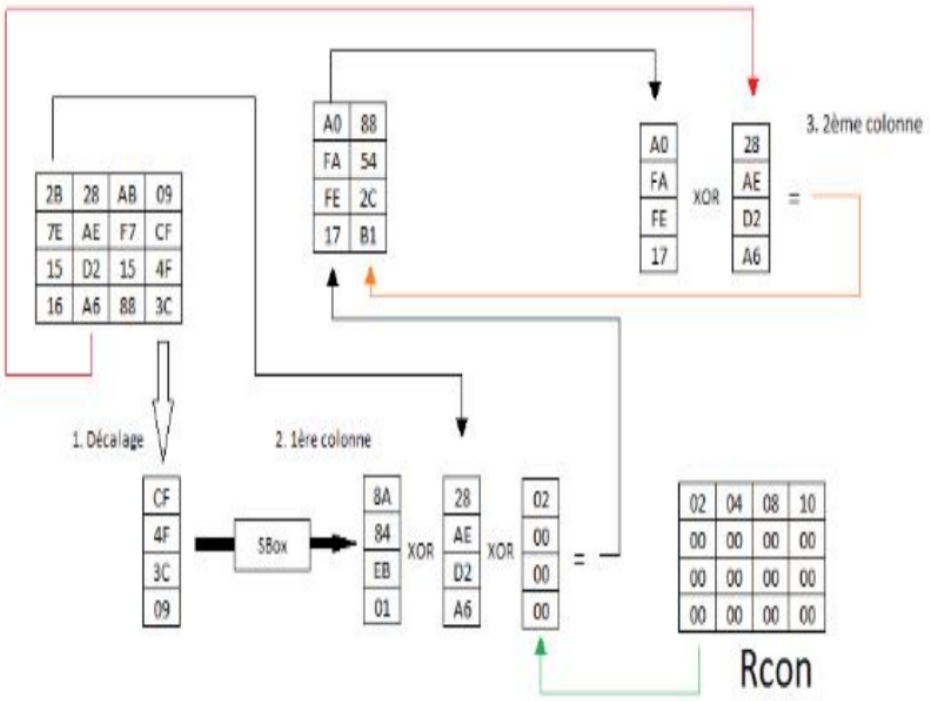

Figure 6: KeyExpansion Fonctionnement

- **AddRoundKey**
  This step will perform a simple xor operation between the key and the state [27]. Once nine rounds have been completed, there is a final round. This round uses the same four steps explained previously with the exception of the "MixColumns" step. Once the final round is over, the message is encrypted. To decipher a message, we simply use the inverse functions of each step, which are generally named InvShiftRows, InvSubBytes, and InvMixColumns.

3.2. Verifying data integrity

To control the integrity of the encrypted data and to ensure that they are not modified during decryption, we chose to work with the MAC protocol [28], because encryption helps protect the confidentiality of the data, but, it does not protect their integrity [22]. A message authentication code or MAC (Message Authentication Code) is a method of calculating a control value which allows the recipient of a message to verify the integrity of received data [18]. The sender calculates the MAC code with the "generate_mac()" function and attaches it to the message that will be send. The recipient receives the message and the associated MAC code. Then it verifies the MAC code with the verification function. If the verification is valid, the message is not modified during transport. If the MAC received during decryption is equivalent to that of encryption, then the data is correct and it is not modified.

Function to generate MAC Key

```
Def generate_mac(key, data) :
h = HMAC.new(Key, digestmod=SHA256)
h.update(data)
return h.digest()
```

- *Step 1:* We will generate a message authentication code (MAC) from a key and specific data. We create a new Hash-based Message Authentication Code (HMAC) object with the specified key and the SHA256 hashing algorithm (digestmod=SHA256). HMAC is a method

for calculating a message authentication code using a cryptographic hash function and a secret key.

- *Step 2:* It updates the HMAC object with the data provided. This adds the data to be used to calculate the MAC.

- *Step 3:* It returns the MAC calculated from the updated data. "h.digest()" calculates the HMAC of the updated data using the specified key and returns the result as bytes.

In summary, this function takes a key and data as input, uses HMAC with SHA256 as a hash function, calculates the MAC of the data with the given key, and returns the result as bytes. This MAC can be used to verify the integrity and authenticity of data during transmission or storage.

4. Result and Discussion

Encryption algorithms such as AES, DES, RSA, SHA or others play a key role in cloud data security. The international data encryption algorithms AES, IDEA, RSA, Blowfish and DES are compared to determine the best security algorithm (see Figure 7).

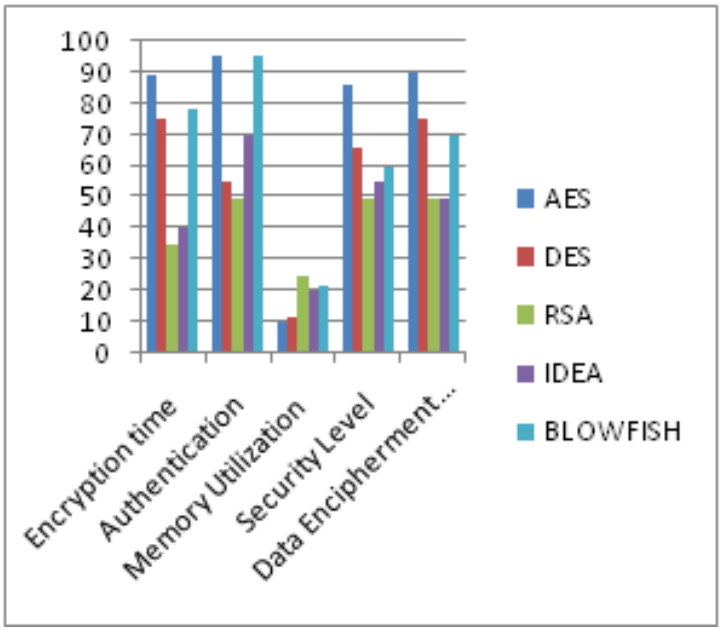

Figure 7: Comparison of algorithms

The evaluation results are shown in Table 1. Table 1 knows that the only asymmetric algorithm is RSA [29-30], but AES, IDEA, Blowfish and DES are symmetric algorithms. IDEA and RSA are the least secure compared to AES, Blowfish and DES. In our study, the AES algorithm takes the least time to encrypt cloud information and can be used to encrypt huge amounts of data with extreme speed, and also the AES algorithm is the best algorithm in terms of encryption parameters. Authentication Blowfish algorithm requires the least memory space, and RSA consumes the most memory and requires a lot of encryption time.

Table 1
The evaluation results

	AES	DES	RSA	IDEA	Blowfish
Plateform	Cloud	cloud	cloud	cloud	cloud
Cipher type	Symmetric	Symmetric	Asymmetric	Symmetric	Symmetric
Security level	Secure for both client and provider	Secure for both client and provider	Only secure for the client	Only secure for the client	Secure for both client and provider
Data encipherment capacity	Encryption of very large amounts of data	Less than AES	Encipherment of small amount of data	Encipherment of small amount of data	Less than AES
Authentication	The best	Less than AES	Less than AES	Less than AES	Identical to AES
Encipherment time	The best	More than AES	needs max time	needs max time	More than AES

5. Conclusion

Information security in the cloud is a major concern for any organization or individuals considering its use. Currently and with the development of technology, encryption remains one of the safest and most reliable solutions to block unauthorized access. Different encryption techniques are used in cloud environments to secure data and reduce hacking to some extent. This study provided an in-depth look at cloud security issues and encryption algorithms used in cloud environments. A literature review was carried out in the field of cloud data security, in which several encryption algorithms were compared to find the optimal security algorithm. The results show that the AES algorithm has high authentication capability and can be used to encrypt huge amounts of data. AES is also faster than other algorithms. Researchers suggest using the AES algorithm to achieve maximum security and speed.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

1. S. Dramé, M. Laurent, L. Castillo, H. GanemCentralized, distributed, and everything in between: reviewing access control solutions for the IoT, ACM Comput. Surv., 54 (2021).
2. J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, B. Fang : A survey on access control in the age of internet of things. IEEE Internet Things J., 7 (2020), pp. 4682-4696
3. N. Kashmar, M. Adda, M. Atieh, H. Ibrahim, A review of access control metamodels,Procedia Comput. Sci., 184 (2021), pp. 445-452
4. S. Xiong, Q. Ni, L. Wang, Q. Wang Sem-acsit: secure and efficient multiauthority access control for IoT cloud storage, IEEE Internet Things J., 7 (2020), pp. 2914- 2927, 10.1109/JIOT.2020.2963899
5. S. Ding, J. Cao, C. Li, K. Fan, H. Li A novel attribute-based access control scheme using blockchain for IoT , IEEE Access, 7 (2019), pp. 38431-38441
6. E. Bertino, P.A. Bonatti, E. Ferrari Trbac: A temporal role-based access control model, Proceedings of the Fifth ACM Workshop on Role-Based Access Control (2000), pp. 21-30

7. A. Yadav, R. Shah :Review on database access control mechanisms and models, Int. J. Comput. Appl., 120 (2015).
8. A. Bhansali, J. Harisha, G. Sinha, "Secure Data Transfer onto Cloud Environment using Diffie-Hellman Key Exchange Algorithm", 2024 International Conference on Inventive Computation Technologies (ICICT), pp.1479-1484, 2024.
9. D.M.F. Mattos, O.C.M.B. Duarte Authflow: authentication and access control mechanism for software defined networking Ann. Telecommun., 71 (2016), pp. 607-615
10. D. Li, W. Peng, W. Deng, F. Gai, A Blockchain-Based Authentication and Security Mechanism for IoT, in: 2018 27th International Conference on Computer Communication and Networks, ICCCN, 2018, pp. 1–6.
11. T. Nguyen, H. Nguyen, T.Nguyen, Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications, Journal of Network and Computer Applications, Volume 226, 2024, 103884, ISSN1084-8045, https://doi.org/10.1016/j.jnca.2024.103884
12. K. Walsh, J. Manferdelli , Intra-cloud and inter-cloud authentication, Cloud computing (CLOUD), 2017 IEEE 10th International Conference on, IEEE (2017), pp. 318-325
13. J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, Y. Park Secure ecc-based three-factor mutual authentication protocol for telecare medical information system IEEE Access, 10 (2022), pp. 11511-11526
14. J Mistry, A Ganesh, R Ramakrishnan, IoT based congenital heart disease prediction system to amplify the authentication and data security using cloud computing, European Chemical (2023).
15. I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure framework enhancing AES algorithm in cloud computing," *Security and Communication Networks*, vol. 2020, pp. 1–16, Sep. 2020, doi: 10.1155/2020/8863345.
16. J. Philip and D. Shah, "Implementing signature recognition system as SaaS on Microsoft azure cloud," in *Data management, analytics and innovation.*, vol. Springer, Springer Singapore, 2019, pp. 479–488.
17. V. Rawat„ D. P Singh, N. Singh, S. Negi,. Heart Disease Prediction Using Machine Learning and Big Data. Big Data, Cloud Computing and IoT: Tools and Applications, 7. (2023)
18. R. Hanumantharaju, K. N. Shreenath, B. J. Sowmya, K. G. Srinivasa, Fog based smart healthcare: a machine learning paradigms for IoT sector. Multimedia Tools and Applications, (2022). 81, 37299-37318.
19. M. Almorsy, J. Grundy, A. S. Ibrahim, (2011) "Collaboration- Based Cloud Computing Security Management Framework" IEEE conference of cloud computing, Washington (DC), pp. 364-371,2011.
20. A.N. Kang, L. Barolli, J.H. Park, Y.S. Jeong, (2013) "A strengthening plan for enterprise information security based on cloud computing", Springer cluster computing, vol. 17, Issue 3, pp. 703-710, 2013.
21. M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025.
22. K. Gai, M. Qiu, and H. Zhao, "Privacy-preserving data encryptionstrategy for big data in mobile cloud computing," *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 1–1, 2017, doi: 10.1109/TBDATA.2017.2705807.
23. B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in *2018 27th Wireless and Optical Communication Conference (WOCC)*, Apr. 2018, pp. 1–5, doi: 10.1109/WOCC.2018.8372705.
24. S. Biswas, R. Roy, M. R. Chowdhury, and A. B. Bhattacharya, "On the advanced strategies of next generation online examination system implementing cloud based standardization: Next generation online examination system," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, Feb. 2016, pp. 834–839, doi: 10.1109/IACC.2016.159.
25. S. Subashanthini and M. Pounambal, "Three stage hybrid encryption of cloud data with penta-layer security for online business users," *Information Systems and e-Business Management*, vol. 18, no. 3, pp. 379–404, Sep. 2020, doi: 10.1007/s10257-019-00419-6.

26. R. C. A. Naidu, A. Srujan, K. Meghana, K. S. Rao, and B. Madhuravani, "Secure privacy preserving of personal health records Using attribute-based encryption in cloud computing," in *First International Conference on Artificial Intelligence and Cognitive Computing*, Springer Singapore, 2019, pp. 59–66.
27. C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, "PPMR: A privacy-preserving online medical service recommendation scheme in eHealthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5665–5673, Jun. 2019, doi: 10.1109/JIOT.2019.2904728.
28. S. Kumar, J. Shekhar, and J. P. Singh, "Data security and encryption technique for cloud storage," in *Conference: CSI-2015;50th Golden Jubilee Annual Convention on Digital Life*, 2018, vol. 729, pp. 193–199, doi: 10.1007/978-981-10-8536-9_19/COVER/.
29. P. More, S. Chandugade, S. M. S. Rafiq, and P. Pise, "Hybrid encryption techniques for secure sharing of a sensitive data for banking systems over cloud," in *2018 International Conference on Advances in Communication and Computing Technology (ICACCT)*, Feb. 2018, pp. 93–96, doi: 10.1109/ICACCT.2018.8529545
30. S. Biswas, R. Roy, M. R. Chowdhury, and A. B. Bhattacharya, "On the advanced strategies of next generation online examination system implementing cloud based standardization: Next generation online examination system," in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, Feb. 2016, pp. 834–839, doi: 10.1109/IACC.2016.159.