ISSN 2278-3083
Volume 8, No.6, November –December 2019
International Journal of Science and Applied Information Technology
Available Online at http://www.warse.org/ijsait/static/pdf/file/ijsait18862019.pdf
https://doi.org/10.30534/ijsait/2019/188620198

# Enhancing The Advanced Encryption Standard (AES) Key Generation using SHA-256 for Secure Data in Cloud Computing

**Rehan Hamdullah Najm[1] , Khalid A. Kaabneh [2]**
[1]Amman Arab university, Amman , Jordan , rehanhamdallah@gmail.com
[2]Amman Arab university , Amman , Jordan , kaabneh@aau.edu.jo

**ABSTRACT**
Information security is one of the most vital areas in the IT sector. Information security can be defined as a science that examines theories and strategies to protect information from all potential threats. From a technical point of view, means, tools, and procedures are required to ensure that information is protected from malicious and accidental internal and external risks. The rapid growth of cloud-based Internet services has led to many serious security attacks of concern to users, Consumers, and companies that use the cloud to store their data are having difficulty maintaining their data, reliable, and confidential Cloud computing has been advanced to deliver IT services so its security is significant as well. This paper fundamentally focuses on two algorithms AES(Advanced Encryption Algorithm) and SHA-256(Secure Hash Algorithms). The aim of the design of the encryption algorithm is to provide security against any unauthorized to data access. The major purpose of this paper is to introduce an idea about the combination of these two algorithms to attain double security to the data stocked inside the cloud and provide encryption speed.

**Key words :** SHA-256 and AES , secure data storage in cloud computing , encryption and decryption data done locally , search encrypted data .

## 1. INTRODUCTION

From data security perspective, which has always been a significant component of quality of service, cloud computing concentrates on new and difficult security threats. Therefore, the data security model should resolve generality cloud security challenges. The data safety model proposed in this research is investigating and providing a security solution for cloud computing, using security algorithms.
One of the risks in cloud computing is that there is no complete security inside the cloud and failure to protect the risks appropriately when using cloud services can lead to higher costs and potential loss of business. Data security remains a source of concern in cloud computing. This concern arises from the fact that sensitive data (text, images, videos, etc.) stored in the cloud is managed by a group of unreliable service providers. There are also many issues with data security in cloud computing(Zhou et al., 2014).
Many types of research have focused on security issues, but the rapid growth of technology and lack of understanding of fundamental problem drove to significant risk to data users(Jing & Qinyuan, 2018). To maintain data in cloud computing is encrypted using various algorithms, encryption means to store and hide the data and capable to provide information, albeit in the presence of the hacker attack(Singh & Sharma, 2015). It can be said that encryption is the science of making data and messages safe so conversion of end-user data to encrypted text cannot read by the hacker attack and that the re-encoding goes back to the original (Waziri et al., 2013).One of the most important encryption goals:
• Confidentiality - A term used to prevent the disclosure of information to unauthorized persons who display or disclose it, and are concerned with a loss of privacy.
• Data integrity- means keeping data from modification by unauthorized persons when someone intentionally or unintentionally deletes or violates the integrity of important data files ,this is a violation of privacy.
• Authentication - is the act of supporting the truth of an attribute of a single part of data alleged true by an entity. In contrast with identification, which points to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually supporting.
AES is a symmetric encryption algorithm. It is useful when we want to encrypt the original text into a confidential text and can also be decrypted and convert back to the original text, for example when we want to send data in e-mail. Decrypting encrypted text is a possibility if we know the correct password. AES is an iterative rather than a Festal encoder. includes a chain of related processes, some of which include replacement of inputs with specific outputs and others include mixed bits about permutations. Therefore, AES remains preferred encryption criterion for governments, banks and high-security systems around the world. (Pancholi, 2016).
Secure hash algorithms (SHA) one-way hash function, The information cannot be retrieved because it does not have a key and is used to block data. it the Length 256 bit (32 bytes) and the block size 512 bit, steps of algorithms 64 steps, word size in bit 32 bit (4 bytes) the Hash algorithm is also one of the

most powerful algorithms that is difficult to break(Arfan, 2017) .

In this research, an algorithm AES was used to encrypt files (texts) while dispensing with the encryption key of this algorithm. AES key generation has many drawbacks such as security and processing time. To overcome this, we propose An Enhancement of Advanced Encryption Standard (AES) Key Generation Using SHA256 to Secure Data in Cloud computing. SHA256 characteristics gave us the speed in generating the key compared to the generating of the private key for algorithm AES other characteristic of using this method is that it is possible to use a file containing a thousand of words that encode it in a fixed size 128 bit by Shorthand, Unlike other algorithms, the words for encryption the key are used.

## 2. BACKGROUND

ADVANCED ENCRYPTION STANDARD (AES)

AES is well-known by its initial name Rijndael is special for the encryption of electronic information construct up by the U.S. National Institute of Standards and Technology (NIST) in 2001(Joan & Vincent, 1999). AES is a subset of the Rijndael assemble cipher generated an improvement by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who presented the proposition to NIST amid the AES determination process. Rijndael a group figures through the various keys and square sizes. For AES, NIST chose three individuals from the Rijndael family, each with a square size of 128 bits, however 3 distinctive key lengths: 128, 192 and 256 bits. AES has been received by the U.S. government and is currently utilized around the world. It supplants the Data Encryption Standard (DES), which was distributed in 1977.The calculation portrayed by AES is a symmetric-key calculation, which means a similar key has been utilized to both encodings with decoding information. at Assembled States, AES was reported by the NIST as U.S. FIPS Bar 197 (FIPS 197) on November 26, 2001 (Rijmen & Joan, 2001). That declaration pursued five-year institutionalization process at which fifteen contending structures be introduced and assessed before the Rijndael figure was chosen as the most appropriate. AES ended up compelling as a national government standard on May 26, 2002, after endorsement by the Secretary of Business. AES is incorporated into the ISO/IEC 18033-3 standard. AES is accessible in various encryption bundles and is the solitary freely available figure endorsed by the National Security Agency (NSA) for best mystery data when utilized an NSA affirmed cryptographic module (Suhaimi, Manji, Goto, & Cheng, 2011).

SECURE HASH ALGORITHM (SHA)

SHA-2 a lot from cryptographic hash capacities structured through the Assembled States National Security Agency (NSA). Are constructed utilizing the Merkle– Damgård structure, of single direction pressure work itself, fabricated utilizing the Davies– Meyer structure of (classified) specific block cipher. SHA-2 incorporates noteworthy changes from its forerunner, SHA-1. The SHA-2 family comprises from six hash capacities with condensations (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-256 and SHA-512 are novel hash capacities figured with 32-bit and 64-bit words, individually. Utilize diverse move sums and added substance constants, however, their structures are generally of all intents and purposes indistinguishable, contrasting just in the number of rounds. SHA-224 and SHA-384 basically cut forms of SHA-256 and SHA-512 individually, figured with various starting qualities. SHA-512/224 and SHA-512/256 have additionally truncated adaptations of SHA-512, however, the underlying qualities are produced to utilizing technique depicted in FIPS Bar 180-4. SHA-2 was distributed in 2001 by NIST a U.S. FIPS. SHA-2 group from calculations is licensed in US patent 6829355. Assembled States has discharged the patent under a sovereignty free permit (Lamberger & Mendel, 2011).

## 3. PROBLEM OF STUDY

Cloud security is one of the most problems and concerns in cloud computing and how to maintain data security and privacy for users in terms of systems processed, viewed or copied from anonymous devices. Some of the issues that pose threat to data security in cloud computing are the use of symmetric encryption algorithms (an algorithm that uses a cryptographic key) if a person can access a secret key that can easily decrypt the text message, the symmetry of the cryptographic algorithm is the most important problem facing the cloud (Bhardwaj, Subrahmanyam, Avasthi, & Sastry, 2016). The problems in cloud computing are the use of identical algorithms, as well as the possibility of knowing the key, in processing the content of the data before sending it to the person requesting the demand, such as whether there is an intruder who has the key, able to handle and modify data content. Security concerns in cloud computing are end-user data security, network traffic, file systems, and device security where encryption works to a certain extent, helping enterprises (Gonzalez et al., 2011).

Many security problems that emerge in the cloud (Bhardwaj et al., 2016):

- Secure data transfer: In a cloud , physical location and access to end-user control are not hosted resources.
- Ensure the safe interface: Ensure the safety of information of hackers through transport, storage and online recovery are not safe.
- Data separation: Privacy case arise when personal data is accessed by cloud service providers or the boundaries between personal data and company data.
- Secure stored data: Query about encryption control and decryption by end-user or cloud service provider.

In symmetric encryption systems, when the key is long, encryption is stronger, but the problem with using large keys it takes longer time to encrypt and decrypt (Sachdev, 2013).In this paper, we propose reduction in encryption time and decryption, as well as increase security because of algorithms symmetric can be broken. This method is proposed using two encryption algorithms, AES 128-bit for data encryption , But

this way is to dispense with the original key for the AES algorithm done is used SHA-256 bit algorithm to encrypt the key.

The research problem can be summed up in the fpllowing fundamental point:

- Need to continuously access data.
- Modification.
- Trust (Admin, Users).

## 4. SIGNIFICANCE OF THE STUDY

The benefits of cloud computing are many, including low cost, easy access to data at any time, and from anywhere in the world. Despite these benefits, however, the disadvantages may pose a significant risk to companies and users as unsafe that the file manager can access the cloud, because It has and all files.

The importance of this research is to secure data locally before sending it to the cloud. In this way, it is data sent through a Safeway and cannot be manipulated, and data can be searched in the cloud remotely in an encrypted form. The most important point that we will adopt in this study is not to share the key with any other party and this gives strength to the proposed method, make it more flexible with the owners of this data, which ensures not to tamper with these data.

The importance of this study stems from a set of research points:

- Encryption / decryption is done locally.
- The use of the encryption algorithm (AES) has also been used to increase security.
- The key is encrypted with an algorithm SHA256.
- Data can be searched and encrypted to increase security and reduce search time.
- When working with algorithms, the encryption speed will increase.

## 5. RELATED WORK

We cite some of the work similar to this research and how data is stored and secured in cloud computing using different types of cryptographic algorithms.

In this paper, they pointed Heroku as a cloud platform, then we implement AES for data security in Heroku. The performance evaluation showed that AES cryptography can be used for data security. furthermore, the delay computation of data encryption illustrates that larger size of data increases the data retard time for encrypting data(Lee, Dewi, & Wajdi, 2018).

This paper fundamentally focuses on two algorithms AES and Blowfish with the aim to design the encryption algorithm to provide security against unauthorized data access. The major purpose of this paper is to make available the idea of the combination of two algorithms to provide double security to data storage in the cloud(Gupta, Saluja, & Tiwari, 2018).

This paper proposes a method for authentication of cellular encryption to provide highly secure authentication. The proposed method uses AES Cryptography for hiding Audio. The authentication key (password) flows into two parts, the first part is used as input text to the encryption process, while the second part is used as a cryptographic key. The encryption key is encrypted using the HMAC-SHA256 hashing algorithm and sent to the server while the second part is encrypted with AES that is encrypted using the x-or encryption algorithm at random. benefit from HMAC uses two paths from the retail account. For the first time, the secret key is used to derive two keys - internal and external. The first part of the algorithm results in internal fragmentation derived from the message and the internal key. The second passageway produces the final HMAC code derived from the result of the internal and external keys. Thus the algorithm provides better immunity against(Salim & Harba, 2018).

Provide a framework to solve the data security problem using both secure retail algorithms and encryption of honey. In addition, remote search is better because it gives us the results of the words we want to find. Data encryption and decryption are performed locally before data is sent to the cloud. We encrypt the original word in an understandable word using a honeycomb encryption that helps intercept hackers. In the decryption process, we rely on the hash table to convert these values to the original words. The goal of this work is to solve the problem by reducing and eliminating risks for data while preserving the benefits of using and enhancing cloud storage (Alhawadi, R & Kaabneh, K 2018).

In the paper, privacy- preserve public audit system for data storage security in cloud computing intended Is done presents the symmetric cryptographic algorithm AES for encrypting data at rest and PGP (Pretty Good Privacy) provide security for the data at motion AES is given as input to the PGP algorithm in the network and PGP provides the second cipher text of given plain text, although, the computational time is increased, the privacy is preserve where data is stored in the cloud using the algorithm AES(Jothy, 2017).

the goal of research to debate the aspect of Cybercrimes will delve into one major example of cybercrime “hacking”. The report will display the application and advancement of technology have magnified different types of offence such as theft crimes and terrorization. Also, this report will show statistical data which will give idea about how far cybercrimes has increased over a term of ten years or more(Kaabneh, 2017).

This paper presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types in spite of the possibility profit achieved from cloud computing, the organizations are slow in accepting it due to security issues, concern and challenges associated with it. Security is one of the major issues which hampers the growth of cloud such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment(Nadeem, 2016).

This paper is a scheme for maintaining data security and integrity using a combination of RSA partial homomorphism and MD5 hashing algorithm. Encryption and decryption are

done by RSA partial algorithm, whereas MD5 hashing algorithm is used to secure data backup (Ora & Pal, 2015).
This paper suggests a framework that allows the generation of a key for specific users with special permissions to access their files that allow the creation of a key for specific users. This framework uses cryptographic algorithms such as AES and RSA. So when a user tries to access files on a cloud using this key, permission will be given by the owner to that user where he is more secure (Chachapara & Bhadlawala, 2013).
In this paper it proposed an unpretentious data security model where data encrypted using (AES) before sending it to the cloud, thus ensuring data confidentiality and security(Sachdev, 2013).
This paper addresses security issues of storing sensitive data in a cloud storage service and the need for users to trust the commercial cloud providers describes the security issues in the cloud storage service The encryption scheme based on the identifier that provides access control has been proposed so that the authorized user can only access the data and that by the authentication (Kaaniche, Boudguiga, & Laurent, 2013).
Encrypting outsourced data by a client is a good stand by to mitigate such solicitude of data confidentiality. Thus, the client preserves the decrypting keys out of reach of the cloud provider. The confidentiality provisioning becomes more complex with flexible data sharing among a group of users. It requires efficient sharing of decrypting keys between different authorized users(Chow et al., 2009).
pointed out this research proposes an adjusted protocol for elliptic curve key exchange based on an elliptic curve over rings, assuming that only the curve E and Fq are public, preservation the base point P secret, which makes attacking the cryptosystem harder by the hacker. Also, we provide embedded authentication, so our protocol does not suffer from the middle man attack (Kaabneh & Al-Bdour,2005).
This research uses a new idea called Heuristic Pursuit on Scrambled Information (HSED), which reduces correspondence overhead on the email server, and it requires no extra calculation with the exception of straightforward computation of a hash work that fills in as the address for passage in the Hash Table (HT). One disadvantage confronted was the impact rate and development time that is identified with the document size, and in managing each report a solitary for looking at the particular catchphrase, which will require a great deal of inquiry time(Qaryouti, Sammour, Shareef, & Kaabneh, 2005).
This paper, sets up a new architecture for security of data storage in multi cloud. Two mechanisms-data encryption and file splitting are used, When a user uploads a file, it is encrypted using the AES encryption algorithm. Then that encrypted file is divided into equal parts according to number of clouds and stored into multicolored. This proposed system reinforces data security in multicolored(Ghavghave & Khatwar, n.d.).
When it comes to data protection in cloud computing, the methods used can be very similar to data protection within a traditional data center. Authentication, identity, access control, encryption, secure deletion, integrity assurance, and data hiding are all data protection methods that can be applied cloud computing. Current research in cloud data protection depends primarily on three main categories:
1) Authentication and Access Control.
2) Encryption.
3) Detect infiltration.

## 6. PROPOSED SCHEMA

The encryption of the key and data in this proposed search is explained in the method described below(1), where the key is encrypted using the SHA-256 algorithm, and the data is encrypted using the encrypted key and AES algorithm. with regarding the decryption process will be the reverse, as shown in figure 2.

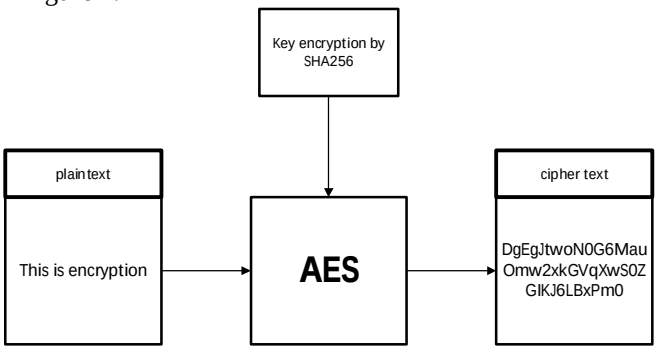


**Figure 1:**. illustrate the proposed encryption method

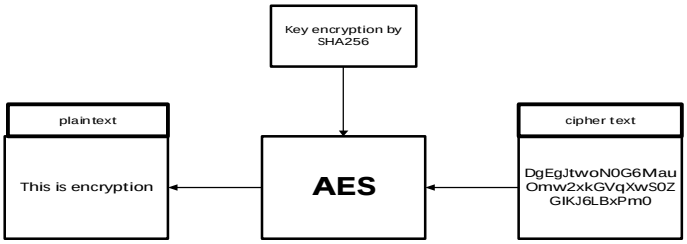


**Figure 2:**. illustrate proposed decryption method

The methodology is a three-stage process: the first stage is encryption where encryption is done as follows:
*A* - Encryption Data:
The key is encrypted using an algorithm SHA256. The algorithm converts a variable-length message to a fixed length of 256 bits, regardless of their original length. Note that any change of any size originally produces a very different discount value than the previous value, or what the job is trying to achieve. After the key is encrypted, the text is encrypted using an AES 128 bit algorithm, shown in figure 3 below.

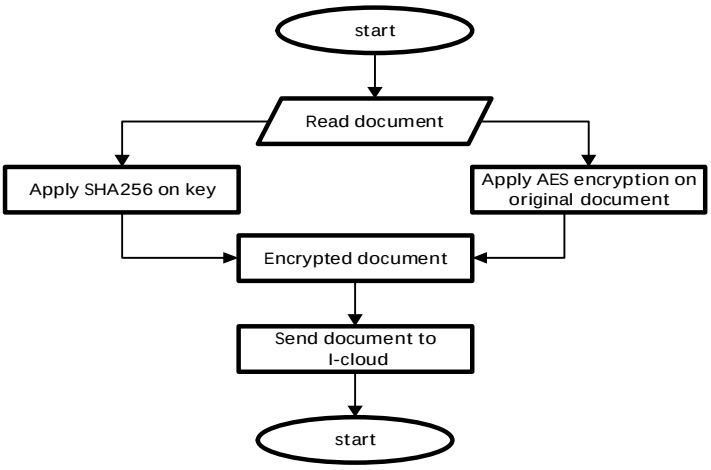


**Figure 3:** step of encryption Data

B - Search Data in I-cloud:

The process of searching encrypted data where, this process will help the user to search the cloud without decrypting the data. Searching for any data in the cloud and providing security for the cloud is difficult as the data in the cloud is in encrypted form. There may be huge data in the cloud that we must work on to decrypt it to get it in readable mode. But this problem can be solved and the search for data is encrypted so that such a system can be implemented which takes less time to search for any keyword related to the required data and is in encrypted form stored on the cloud.

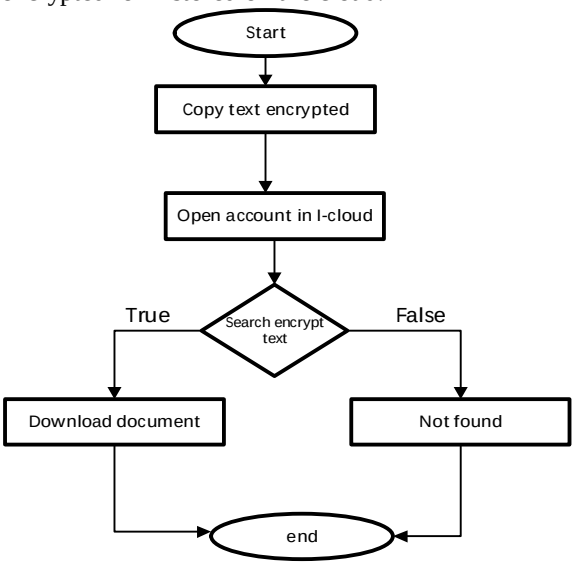


**Figure 4:**. Step of the search Data in I-cloud

C- Decryption Data:

The data is decoded using the same encrypted data key and because AES a symmetric algorithm, the algorithm used to encrypt the key is a vector algorithm, the following figure illustrates the decryption process.

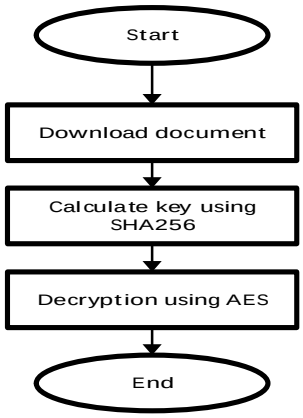


**Figure 5:** Steps in Decryption Data

## 7. SIMULATION RESULTS

The number of times the hacker needs to break the key in this proposal is as explained in the following equation:

a) AES = brute force attack: $2^{256}$

Then key length = 256 bit (original key)
$2^{256}$ = Time to break the key (original key)
The number is fictional and cannot be calculated on the calculator.

b) Proposed method = brute force attack: $2^{256(256)}$

Then key length = 256 bit (original key)
$2^{256}$ = (Time to break the key original key) $^{256}$
Here will be the first product to break the key which is a fantastic number but in addition to that time will be here to break the key is too large because the output will have to force 256 because of the use of SHA-256.
Either from aspect measure, key encryption speed may be the speed of the encryption key was measured on a large set of files, As shown in the figure below.

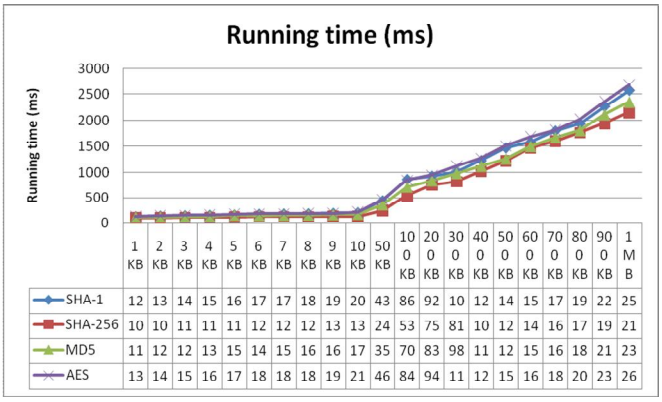


**Figure 6:** Measure key encryption speed

## 8. CONCLUSION

Here is presented the final result and the conclusions drawn from this paper. The benefit of the proposed method is to develop the AES encryption in terms of key strength and use it

to store data on the cloud where the results are very encouraging**.** Through the tests, we found that the implementation time for the proposal is lower. On the other hand, we stress that the proposed method does not involve the sharing of the key between more than one user. In the proposed method, the SHA-256 is applied to the key because it does not contain a collision, and also helps in using a file or a set of words, not like the other algorithms one word or a certain number of bits because whatever the size of data or words will get a fixed length is 256 bits. It is the benefits of Hash that help in detecting any modification the data gets. The time needed to break the key in the proposed method is twice as much as the time in AES so this helps to protect the data more forcefully**.**

**REFERENCES**


1. Arfan, M. (2017). Mobile cloud computing security using cryptographic hash function algorithm. *Proceedings - 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2016*, 1–5.https://doi.org/10.1109/ICITACEE.2016.7892480
2. Alhawadi,R & Kaabneh,K (2018).keyword search on encrypted data in I-cloud computing. Master thesis in amman arab university
3. Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security Algorithms for Cloud Computing. *Procedia Computer Science*, *85*(Cms), 535–542. https://doi.org/10.1016/j.procs.2016.05.215
4. Chachapara, K., & Bhadlawala, S. (2013). Secure sharing with cryptography in cloud computing. *2013 Nirma University International Conference on Engineering (NUiCONE)*, 1–3. https://doi.org/10.1109/NUiCONE.2013.6780085
5. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud : Outsourcing Computation without Outsourcing Control, 85–90.
6. Ghavghave, R. S., & Khatwar, D. M. (n.d.). Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm, 157–161.
7. Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 231–238. https://doi.org/10.1109/CloudCom.2011.39
8. Gupta, U., Saluja, S., & Tiwari, T. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. *International Journal of Recent Research Aspects*, *5*(1), 55–61. Retrieved from https://liverpool.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129311331&site=eds-live&scope=site
9. Jothy, K. A. (2017). Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm, *8*(6), 582–585.
10. Kaabneh, P. K. (2017). Cybercrimes , Real or Meth ?, *7*(1), 23–29.
11. Kaaniche, N., Boudguiga, A., & Laurent, M. (2013). ID based cryptography for cloud data storage. *IEEE International Conference on Cloud Computing, CLOUD*, 375–382. https://doi.org/10.1109/CLOUD.2013.80
12. Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018). Data security in cloud computing using AES under HEROKU cloud. *2018 27th Wireless and Optical Communication Conference, WOCC 2018*, 1–5. https://doi.org/10.1109/WOCC.2018.8372705
13. Nadeem, M. A. (2016). Cloud Computing: Security Issues and Challenges. *Journal of Wireless Communications*, *1*(1). https://doi.org/10.21174/jowc.v1i1.73
14. Qaryouti, J., Sammour, G., Shareef, M., & Kaabneh, K. (2005). Heuristic Search on Encrypted Data (HSED). *Amman, Jordan*, (August).
15. Sachdev, A. (2013). Enhancing Cloud Computing Security using AES Algorithm. *International Journal of Computer Applications*, *67*(9), 19–23. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.5675&rep=rep1&type=pdf
16. Salim, E., & Harba, I. (2018). Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography. *Iraqi Journal of Science*, *59*(1C), 600–606. https://doi.org/10.24996/ijs.2018.59.1C.17
17. Abualigah, L. M. Q. (2019). Feature selection and enhanced krill herd algorithm for text document clustering. Berlin: Springer.
18. Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security Algorithms for Cloud Computing. Procedia Computer Science, 85(Cms), 535–542. https://doi.org/10.1016/j.procs.2016.05.215
19. Chachapara, K., & Bhadlawala, S. (2013). Secure sharing with cryptography in cloud computing. 2013 Nirma University International Conference on Engineering (NUiCONE), 1–3. https://doi.org/10.1109/NUiCONE.2013.6780085
20. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud : Outsourcing Computation without Outsourcing Control, 85–90.
21. Ghavghave, R. S., & Khatwar, D. M. (n.d.). Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm, 157–161.
22. Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. 2011 IEEE Third

International Conference on Cloud Computing Technology and Science, 231–238. https://doi.org/10.1109/CloudCom.2011.39
23. Gupta, U., Saluja, S., & Tiwari, T. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. International Journal of Recent Research Aspects, 5(1), 55–61. Retrieved from https://liverpool.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129311331&site=eds-live&scope=site
24. Jothy, K. A. (2017). Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm, 8(6), 582–585.
25. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2019). Modified Krill Herd Algorithm for Global Numerical Optimization Problems. In *Advances in Nature-Inspired Computing and Applications* (pp. 205-221). Springer, Cham.
26. Kaaniche, N., Boudguiga, A., & Laurent, M. (2013). ID based cryptography for cloud data storage. IEEE International Conference on Cloud Computing, CLOUD, 375–382. https://doi.org/10.1109/CLOUD.2013.80
27. Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018). Data security in cloud computing using AES under HEROKU cloud. 2018 27th Wireless and Optical Communication Conference, WOCC 2018, 1–5. https://doi.org/10.1109/WOCC.2018.8372705
28. Nadeem, M. A. (2016). Cloud Computing: Security Issues and Challenges. Journal of Wireless Communications, 1(1). https://doi.org/10.21174/jowc.v1i1.73
29. Qaryouti, J., Sammour, G., Shareef, M., & Kaabneh, K. (2005). Heuristic Search on Encrypted Data (HSED). Amman, Jordan, (August).
30. Sachdev, A. (2013). Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications, 67(9), 19–23. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.5675&rep=rep1&type=pdf
31. Salim, E., & Harba, I. (2018). Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography. Iraqi Journal of Science, 59(1C), 600–606. https://doi.org/10.24996/ijs.2018.59.1C.17
32. Arfan, M. (2017). Mobile cloud computing security using cryptographic hash function algorithm. *Proceedings - 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2016*, 1–5. https://doi.org/10.1109/ICITACEE.2016.7892480
33. Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security Algorithms for Cloud Computing. *Procedia Computer Science*, *85*(Cms), 535–542. https://doi.org/10.1016/j.procs.2016.05.215
34. Chachapara, K., & Bhadlawala, S. (2013). Secure sharing with cryptography in cloud computing. *2013 Nirma University International Conference on Engineering (NUiCONE)*, 1–3. https://doi.org/10.1109/NUiCONE.2013.6780085
35. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud : Outsourcing Computation without Outsourcing Control, 85–90.
36. Ghavghave, R. S., & Khatwar, D. M. (n.d.). Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm, 157–161.
37. Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 231–238. https://doi.org/10.1109/CloudCom.2011.39
38. Gupta, U., Saluja, S., & Tiwari, T. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. *International Journal of Recent Research Aspects*, *5*(1), 55–61. Retrieved from https://liverpool.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=129311331&site=eds-live&scope=site
39. Jothy, K. A. (2017). Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm, *8*(6), 582–585.
40. Kaabneh, P. K. (2017). Cybercrimes , Real or Meth ?, *7*(1), 23–29.
41. Kaaniche, N., Boudguiga, A., & Laurent, M. (2013). ID based cryptography for cloud data storage. *IEEE International Conference on Cloud Computing, CLOUD*, 375–382. https://doi.org/10.1109/CLOUD.2013.80
42. Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018). Data security in cloud computing using AES under HEROKU cloud. *2018 27th Wireless and Optical Communication Conference, WOCC 2018*, 1–5. https://doi.org/10.1109/WOCC.2018.8372705
43. Nadeem, M. A. (2016). Cloud Computing: Security Issues and Challenges. *Journal of Wireless Communications*, *1*(1). https://doi.org/10.21174/jowc.v1i1.73
44. Qaryouti, J., Sammour, G., Shareef, M., & Kaabneh, K. (2005). Heuristic Search on Encrypted Data (HSED). *Amman, Jordan*, (August).
45. Sachdev, A. (2013). Enhancing Cloud Computing Security using AES Algorithm. *International Journal of Computer Applications*, *67*(9), 19–23. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.5675&rep=rep1&type=pdf
46. Salim, E., & Harba, I. (2018). Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography. *Iraqi Journal of Science*, *59*(1C), 600–606. https://doi.org/10.24996/ijs.2018.59.1C.17