

# CRYPTOGRAPHY IN CLOUD COMPUTING FOR DATA SECURITY AND NETWORK SECURITY

Wissam Zaki Mizyad Al-Humadi

Computer Center, University of Basrah, Iraq.

wissam.mizyad1973@gmail.com

**Abstract:** Cloud computing is a very useful technology in our daily life, this computing uses the Internet to provide applications and also to transfer and maintain data , it is imperative to provide an environment that protects applications and data within this cloud , networks have to be protocols that use strong algorithms to protect them this paper discusses some of them and compares them with others, data security and encryption is considered one of the most important discoveries, despite its development in the old days completely separately now that reality showed a close connection between them.

**Keywords:** encryption, data, network, security, protocols.

## I. INTRODUCTION

Cloud computing technology is a model for enabling access to a shared network of computing resources, it has become a very popular topic of research and important issues such as electricity and water , conveyor networks are essential in them, as they must be protected, in this paper the methods of protection were thoroughly followed and studied the first appearance of protection, its disadvantages were discussed and how mistakes made were avoided, a comparison was also made between two types of encryption, transfer data and how it is protected by means of encryption, as it is necessary to protect it. Here, how data is protected has also been clarified and a model of algorithms has been taken, this algorithm will show how it is encrypted and protected from attacker this algorithm was applied to the python program, and the results were obtained on encoding and decoding the data, and detailing this was done by codes.

## II. CLOUD COMPUTING SECURITY

A computing cloud can be expressed in order to provide or connect computer services and resources (Data bases, analyzes, storage spaces ...).

And all of these operations are done by the Internet, and that by providing interfaces to manage the services provided by the cloud computing This is usually over the web.

This computing cloud has several advantages that we can mention.

- **Provide self-service :**The user can specify the resources required to operate and start working without the need to wait for settings from the network administrator.
- **Flexibility:** User can increase and decrease resources as needed.
- **Pay to use:** Meaning that the service provider calculates only the resources that have been used, and only these resources are accounted for.
- **Flexibility in transportation:** User can transfer data from one cloud to another easily.

In the past (the nineties) your data was on your computer or if you worked in a company that was stored in the servers of that company, and everything changed when the cloud appeared. Your data can be located anywhere, and the same goes for your applications That is why it became more difficult for data security and cloud security became necessary.

**Cloud security** is a complete set of technologies and protocols that protect cloud computing data, and this process is done by encrypting every step within the cloud that can be summarized into

- 1- Encryption key management :This tool enables administrators to provide their own encrypted keys or they can request to create a key for them to protect their databaseIt supports key files, key encryption PFX and BYOK.
- 2- Client-side encryptionThis means that user data is encrypted before it is sent the text of the key used for encryption is not only saved locallySo that the user data is safe, and the original data cannot be decoded even if the data is leaked.
- 3- Cloud server encryptionContent-aware coding and coordinated coding are common encryption methodsA content-aware program uses the data or formats and codecs used to prevent data leakageBased on policy settings such as automatically encrypting the credit card number when sent to law enforcement by email.
- 4- Cloud password machine serviceA cloud server encryption device is a hardware encryption device that uses a virtualization method to create multiple virtual encryption devices.
- 5- Key management servicesExisting cloud service providers can provide encryption key schemes to protect the development of cloud-based applications and services, or they can leave this protection to users. As cloud service providers advance towards solutions that support strong key management.
- 6- Data encryption:encryption technology is used to protect the security of data during storage and transmission (link encryption technology). For storage technicians, the encryption systems and technologies commonly encountered are storage backgrounds that support encryption, such as cryptography. Disk or storage encryption.

### III. DATA ENCRYPTION AND PROTECTION BY PROGRAMMING LANGUAGE

Encryption is a method of encoding a message in a form that is not readable by unauthorized users, this is done by using algorithms that transform the original data.

Here, a distinction must be made between data masking and data encryption

Data masking is a technique for hiding communication by masking the confidential message into a fake one.

The difference is that Data masking is a science that deals with how a connection can be hidden whereas, data encryption is the science of transforming the content of communication and making it obscure.

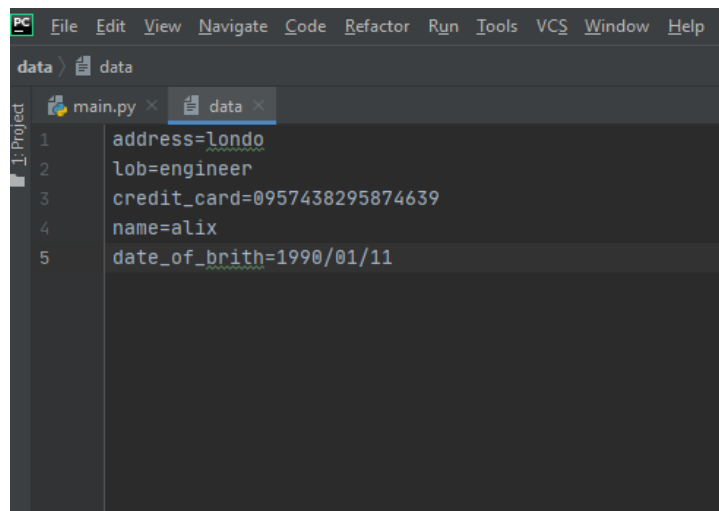
Therefore, any data must be encrypted before entering the cloud computing because its detection would have unsatisfactory results for the user, whether it was a credit card number or a bank account or other.

There are many encryption methods from different programs, but we will use Python for encryption, Python has many encryption methods such as (RSA cipher) or SDES or other.

But here to encrypt the data we will take the type encode and decoding, but this type needs database, this type is hashlib (MD5).

steps First we open the program and create a file that contains all the data to be encrypted before sending on cloud computing Such as address, work, credit card number, name, date of birth

As in the figure below.



```
PC File Edit View Navigate Code Refactor Run Tools VCS Window Help
data > data
main.py x data x
1 address=Londo
2 lob=engineer
3 credit_card=0957438295874639
4 name=alix
5 date_of_brith=1990/01/11
```

Fig1 : The data to be encrypted

### Work stepsfor encryption

1- From hashlib import \*

This code means that the hashlib was called give a \* This means calling out everything.

2- File=input (“Enter the file name:”)

Calling file name from outside means by input it takes data.

3- With open (file, mode=’r’) as f:

Here the filename is called and given a commandmode = r,this file means readable.

4- For line in f:

call up for loop working on this file and for every line in this file.

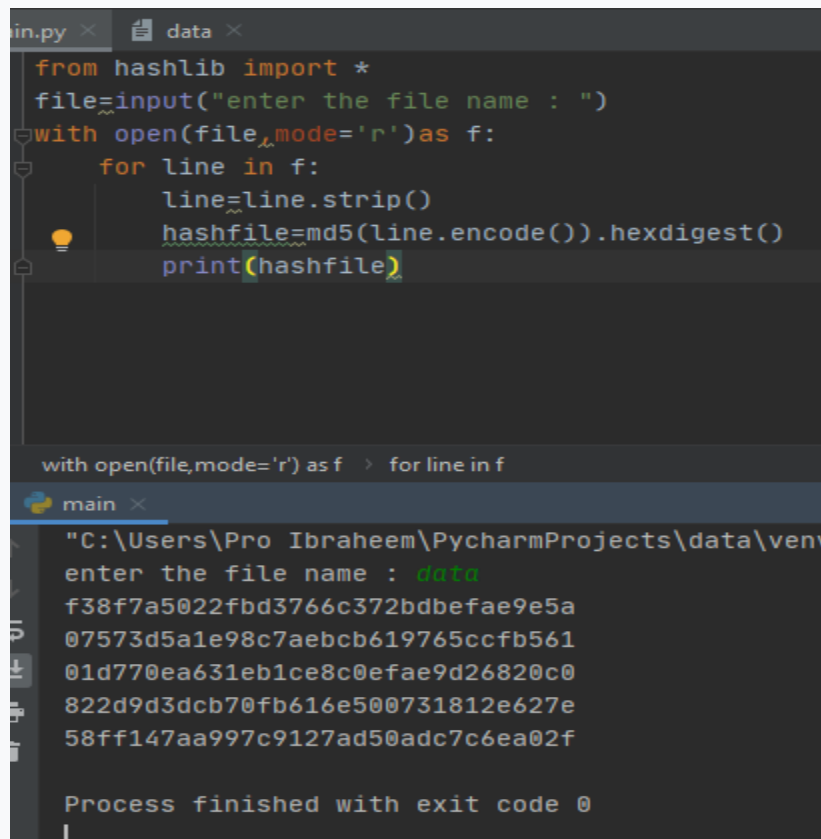
5- Line=line. Strip ()

Here the task of this function is to format the data inside the file.

6- Hashlib=md5(line. Encode ()).hexdigest ( )

Here means the MD5 function was called That takes the data to be encoded and continues until we get its final imagehexdigest ( ).

After applying this program and entering into it all the data that we wanted to encrypt It shows us the results in a way that is not readable or understandable. As in the figure below.



```
in.py x data x
from hashlib import *
file=input("enter the file name : ")
with open(file,mode='r')as f:
    for line in f:
        line=line.strip()
        hashfile=md5(line.encode()).hexdigest()
        print(hashfile)

with open(file,mode='r') as f > for line in f

main x
"C:\Users\Pro Ibraheem\PycharmProjects\data\venv
enter the file name : data
f38f7a5022fbd3766c372bdbefae9e5a
07573d5a1e98c7aebcb619765ccfb561
01d770ea631eb1ce8c0efae9d26820c0
822d9d3dcb70fb616e500731812e627e
58ff147aa997c9127ad50adc7c6ea02f

Process finished with exit code 0
```

Fig2:Data encryption results

### Work stepsfor decryption

Now we are decryptionand here we take the same previous exampleand also work by hashlib and the way it works is through the databasethe database contains encrypted data when we give encrypted data, it takes and searches the database for something that matches it and when he finds it, he takes the original word for it with this, the encryption is unlocked The following is an explanation of decryption by the application in the program.

1- From hashlib import \*

This code means that the hashlib was called give a \* This means calling out everything.

2- Word=input ("Enter the hash here: ")

Here we have given a word and input to enter the data to be encrypted.

3- File=input ("Enter the file name:")

Calling file name from outside means by input it takes data.

4- With open (file, mode='r') as f:

Here the filename is called and given a command mode = r, this file means readable.

5- For line in f:

call up for loop working on this file and for every line in this file.

6- Line=line. Strip ()

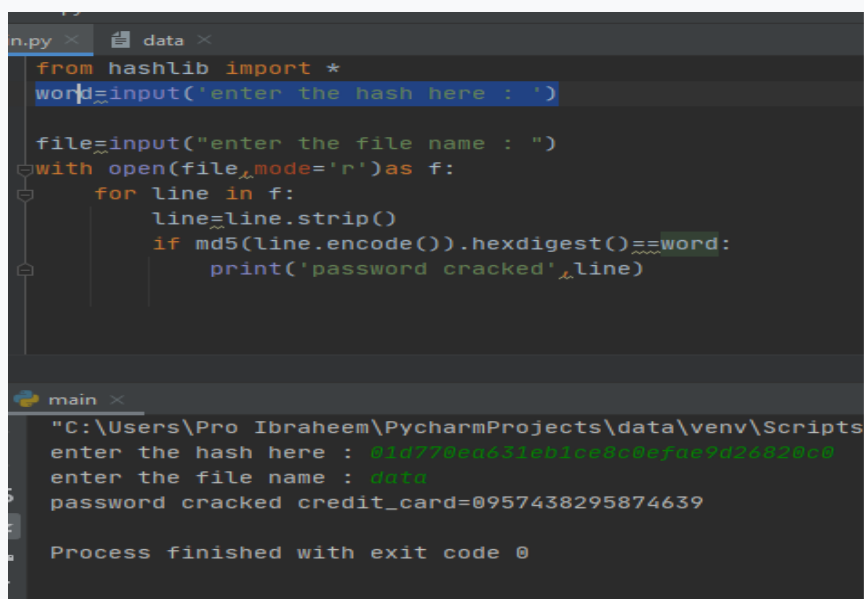
Here the task of this function is to format the data inside the file.

7- If md5(line. Encode ()).hexdigest () ==word:

At this step the if conditional was used and the condition becomes if every line in the database after encryption equals the word print.

8- Print ('password cracked ', line).

As in the figure below.



```
n.py x data x
from hashlib import *
word=input('enter the hash here : ')

file=input("enter the file name : ")
with open(file,mode='r')as f:
    for line in f:
        line=line.strip()
        if md5(line.encode()).hexdigest()==word:
            print('password cracked ',line)

main x
"C:\Users\Pro Ibraheem\PycharmProjects\data\venv\Scripts
enter the hash here : 01d770ea631eb1ce0c0ef0e9d24d20c0
enter the file name : data
password cracked credit_card=0957438295874639

Process finished with exit code 0
```

Fig3: Data decryption results

#### IV. NETWORK ENCRYPTION AND PROTECTION

Most people do not realize that we rely on encrypted networks every time we use the Internet, and this thing is done by many algorithms that encode and decipher cipher.

For this matter we will take three levels of encryption and we review the most important characteristic of it.

1- WEP (wired equivalent privacy) It is the first level and types of encryption that he used to protect Wi-Fi in 1999, And it is one of the weakest levels of encryption ever and the easiest to penetrate, The reason for this is the reluctance of network device manufacturers to impede users and ease their communication with networks at the expense of increasing protection and encryption.

2- WPA (Wi-Fi protected access) After the system vulnerability that occurred with the old coding, a new type must have appeared in 2003, The most important characteristic of this

encryption is the increase in the length of the encryption key to 256 bits, He passed through many stages and names of them WPA\_PSK (Pre-shared key) and also WPA-TKIP (temporal key integrity protocol), Hackers have a desire to prove the weakness of the new encryption system, and although the time is long and its penetration is difficult, it has already been hacked.

3- WPA2 (wireless protected access 2 )In 2006, wp entered work, a level of encryption that is the best among the three levels, and it came to fix the gaps that occurred in the system WPA Although it is the strongest level of encryption now and filling system vulnerability, it depends on the WPA system, which came in the first place, depending on the mother system WEP.

If we talked about the most secure protocols, WPA2 is the first, as for encryption, AES with CCMP is the most secure encryption. WPA2 start using the algorithm AES with CCMP instead of TKIP, Previously in WPA it was AES optional, but in WPA2 it was AES mandatory.

**AES**(advanced encryption standard)

It is considered one of the most important ways to encode important data in a WPA2 protocol.to explain the algorithm in simple terms that it takes a plain text and turns it into an encrypted text and it seems that the cipher is advised as a random string of characters to an observer who does not have the encryption key.the device or person on the other end of the transmitter contains a key that decrypts the data to facilitate viewing, And the device from which the transmission is directed contains the first key that encrypts before sending, encryption levels are heh (128, 192, 256 bits) even the smallest level of 128 is theoretically unbreakable because current computing power takes more than 100 billion years to find the correct solution to the cryptographic algorithm.

AES protection properties

- 1- Protection :AES algorithms have the ability to resist attacks better than others.
- 2- Implementation: the as algorithms are flexible as well as easy to implement.
- 3- the cost: very few.

Comparison between DES and AES

DES (dataencryption standard) it is an outdated method instead of encrypting the data so that the information cannot be read by other people who may be intercepting the traffic, it is considered very old and has been replaced by AES.

(advanced encryption standard) the following will explain the difference below.

AES	DES	
1999	1977	Development
(128, 192, 256 bits)	56 bits	Key length
It is considered safe	Prove that not enough	Protection
128 bits	64 bits	Section size

Fig4: Comparison between DES and AES

## V. CONCLUSION

The services provided by any cloud computing model are closely linked to mobility and thus depend heavily on continuous internet connectivity, it needs secure networks to move it, and so does its data security that is why we did this research and produced results regarding encryption and decryption of data, and gave examples that could be applied.

Therefore, we recommend me

- Create a secure cloud computing community, to share ideas and collaborate.
- Making the subject of cloud computing and its protection a basic subject taught in all study stages.
- Developing protection methods and making them easier to learn and implement.

## VI. REFERENCES

- [1] Beloglazov, A. and Buyya, R., 2012. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers. *Concurrency and Computation: Practice and Experience*, 24(13), pp.1397-1420.
- [2] Zeller, M., Grossman, R., Lingenfelder, C., Berthold, M.R., Marcade, E., Pechter, R., Hoskins, M., Thompson, W. and Holada, R., 2009, June. Open standards and cloud computing: KDD-2009 panel report. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 11-18).
- [3] Vu, Q.H., Pham, T.V., Truong, H.L., Dustdar, S. and Asal, R., 2012, March. Demods: A description model for data-as-a-service. In *2012 IEEE 26th International Conference on Advanced Information Networking and Applications* (pp. 605-612). IEEE.

- [4] Dillon, T., Wu, C. and Chang, E., 2010, April. Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). Ieee.
- [5] Clark, C., Fraser, K., Hand, S., Hansen, J.G., Jul, E., Limpach, C., Pratt, I. and Warfield, A., 2005, May. Live migration of virtual machines. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2* (pp. 273-286).
- [6] Li, C., Zhang, Y. and Xie, E.Y., 2019. When an attacker meets a cipher-image in 2018: A year in review. *Journal of Information Security and Applications*, 48, p.102361.
- [7] Agrawal, R., Kiernan, J., Srikant, R. and Xu, Y., 2004, June. Order preserving encryption for numeric data. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data* (pp. 563-574).
- [8] Dobkin, D., Jones, A.K. and Lipton, R.J., 1979. Secure databases: Protection against user influence. *ACM Transactions on Database systems (TODS)*, 4(1), pp.97-106.
- [9] Bourke, P.D. and Dalenius, T., 1976. Some new ideas in the realm of randomized inquiries. *International Statistical Review/Revue Internationale de Statistique*, pp.219-221.
- [10] Chee, M., Yang, R., Hubbell, E., Berno, A., Huang, X.C., Stern, D., Winkler, J., Lockhart, D.J., Morris, M.S. and Fodor, S.P., 1996. Accessing genetic information with high-density DNA arrays. *Science*, 274(5287), pp.610-614.
- [11] Deaton, R.J., Murphy, R.C., Garzon, M.H., Franceschetti, D.R. and Stevens Jr, S.E., 1996, June. Good encodings for DNA-based solutions to combinatorial problems. In *DNA Based Computers* (pp. 247-258).
- [12] Ezziane, Z., 2005. DNA computing: applications and challenges. *Nanotechnology*, 17(2), p.R27.
- [13] Abdelhakim, M., Lightfoot, L.E., Ren, J. and Li, T., 2013. Distributed detection in mobile access wireless sensor networks under byzantine attacks. *IEEE Transactions on Parallel and Distributed Systems*, 25(4), pp.950-959.
- [14] Yue, X., Chen, W. and Wang, Y., 2009, November. The research of firewall technology in computer network security. In *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)* (Vol. 2, pp. 421-424). IEEE.
- [15] Lalitha, N. and Manimegalai, P., 2014. VP Muthu kumar, M. Santha,|| Efficient data hiding by using AES and advance Hill cipher algorithm||. *International journal of research in computer applications and Robotics*, 2(1).
- [16] Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M. and Rao, N., 2013. Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*, 51(7), pp.36-43.
- [17] Kaushik, S. and Singhal, A., 2012. Network security using cryptographic techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(12), pp.105-107.
- [18] Jasuja, B. and Pandya, A., 2015. Crypto-compression system: an integrated approach using stream cipher cryptography and entropy encoding. *International Journal of Computer Applications*, 116(21), pp.34-41.



- [19] Sadkhan, S.B., 2004, April. Cryptography: Current status and future trends. In *Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.* (pp. 417-418). IEEE.
- [20] Varol, N., Aydogan, A.F. and Varol, A., 2017, April. Cyber attacks targeting Android cellphones. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-5). IEEE.
- [21] Tayal, S., Gupta, N., Gupta, P., Goyal, D. and Goyal, M., 2017. A Review paper on Network Security and Cryptography. *Advances in Computational Sciences and Technology*, 10(5), pp.763-770.
- [22] Choo, K.K.R., Domingo-Ferrer, J. and Zhang, L., 2016. Cloud Cryptography: Theory, Practice and Future Research Directions. *Future Gener. Comput. Syst.*, 62(C), pp.51-53.
- [23] Hu, Y.C., Lo, C.C. and Chen, W.L., 2016. Probability-based reversible image authentication scheme for image demosaicking. *Future Generation Computer Systems*, 62, pp.92-103.